CRC Press
Taylor & Francis Group

From Street-smart to Web-wise®

A Cyber Safety Training Program Built for Teachers and Designed for Children (Book 4)

Al Marcella, Brian Moore,
and Madeline Parisi

"*From Street-smart to Web-wise*® is a game-changer for digital literacy education. This series equips educators with the tools to transform students into savvy, ethical digital citizens. With ready-to-use lessons on cybersecurity, online ethics, and AI, it's an essential resource for preparing the next generation to thrive in our tech-driven world. Timely, comprehensive, and critically important."

— **Nell Watson**, *IEEE AI Ethics Maestro, Belfast, Northern Ireland*

"As someone who spends a lot of time teaching healthy relationships to children and teens, this book is a breath of fresh air. It doesn't adopt the 'quick fix' mentality that our current culture is so often obsessed with. Instead, it thoughtfully, clearly, and consistently addresses the underlying issues contributing to the online vulnerabilities of our youth. It equips teachers and caregivers with the tools to genuinely prepare the next generation, all while promoting trust without resorting to fear. Well done!"

— **Morrisa Berkley**, *Coach, Advocate, and Founder of Love One*

"In the realm of cybersecurity, where technology, processes, and people all play crucial roles, the human element is often considered the weakest link. This is especially true for children, who are at greater risk due to their limited experience in navigating the digital world. As both a cybersecurity professional and a father of a 16-year-old, I am delighted to see books like this that tackle these vital issues head-on. This invaluable resource empowers educators to create awareness about cyber safety and cybersecurity among children. It comprehensively covers fundamental topics such as secure passwords, digital footprints, and Personally Identifiable Information (PII), while also addressing emerging challenges like AI and its associated risks. Importantly, it presents all this information in an easy-to-understand way, making it accessible for young audiences."

— **Mathias Conradt,** *Principal Solutions Engineer at Snyk, Stuttgart, Germany*

"To foster our student's success in a digital era, it's important that we exemplify proper usage ourselves and give them chances to apply character education principles in digital spaces, which now encompass the dynamic landscape of AI. *From Street-smart to Web-wise™: A Safety Training Manual Built for Teachers and Designed for Children* serves as a resource, offering educators a pathway to integrate these two spheres and facilitate meaningful learning experiences."

— **Kristina Lodes,** *Digital Learning Coach, Saint Louis, Missouri, USA*

"There are two things that delight me about this book. Firstly, the knowledge, experience, and passion of those who created it. Secondly, the support it gives to educators."

— **Wendy Goucher,** *MSc (Res), FBCS, Cyber Consultant and Author, Scotland, UK*

“The lesson plans are creative, thorough, and easy to use without relying on scare tactics or being overly prescriptive.”

— **John F. Boyce**, *Head-People Development, AMSOIL, Inc., USA*

“Online safety is one of the top concerns for educators and parents.”

— **Christine Burke**, *Elementary School Principal, St. Louis, Missouri, USA*

From Street-smart to Web-wise®

Our seventh and eighth graders are now "officially" teens, and online activities are second nature. *From Street-smart to Web-wise®: A Cyber Safety Training Manual Built for Teachers and Designed for Children* isn't just another book. Teachers will find this book to be a road map to navigate the digital landscape safely, with confidence and care, as their critical job of ensuring students' safety in a digital world expands.

Dive into engaging content that illuminates the importance of cyber safety, not only in our classrooms but extending into the global community.

Written by authors who are recognized experts in their respective fields, this accessible manual is a timely resource for educators. Each chapter is filled with practical examples and teacher tips, stimulating discussion points, and ready-to-use lesson plans tailored for students in seventh and eighth grades. Regardless of your technology skill level, this book will provide you with the guidance and the tools you need to make student cyber safety awareness practical, fun, and impactful.

Parents consider educators their partners in creating cyber-secure spaces. This book stands as a framework of commitment to that partnership whether you are in middle school environment or in a child-serving agency. It confirms proactive steps in equipping our young learners with the awareness and skills they need to tread the digital world securely.

By choosing *From Street-smart to Web-wise®: A Cyber Safety Training Manual Built for Teachers and Designed for Children*, you position yourself at the forefront of educational guardianship, championing a future where our children can explore, learn, and grow online without fear. Join us on this journey to empower the next generation—one click at a time!

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

From Street-smart to Web-wise®

A Cyber Safety Training Program Built for Teachers and Designed for Children (Book 4)

Al Marcella, Brian Moore, and Madeline Parisi

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Designed cover image: Shutterstock Image ID 600603497

First edition published 2026
by CRC Press
2385 NW Executive Center Drive, Suite 320, Boca Raton FL 33431

and by CRC Press
4 Park Square, Milton Park, Abingdon, Oxon, OX14 4RN

CRC Press is an imprint of Taylor & Francis Group, LLC

© 2026 Al Marcella, Brian Moore and Madeline Parisi

Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. The authors and publishers have attempted to trace the copyright holders of all material reproduced in this publication and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Except as permitted under U.S. Copyright Law, no part of this book may be reprinted, reproduced, transmitted, or utilized in any form by any electronic, mechanical, or other means, now known or hereafter invented, including photocopying, microfilming, and recording, or in any information storage or retrieval system, without written permission from the publishers.

For permission to photocopy or use material electronically from this work, access www.copyright.com or contact the Copyright Clearance Center, Inc. (CCC), 222 Rosewood Drive, Danvers, MA 01923, 978-750-8400. For works that are not available on CCC please contact mpkbookspermissions@tandf.co.uk

Trademark notice: Product or corporate names may be trademarks or registered trademarks and are used only for identification and explanation without intent to infringe.

ISBN: 978-1-032-73179-7 (hbk)
ISBN: 978-1-032-73864-2 (pbk)
ISBN: 978-1-003-46637-6 (ebk)

DOI: 10.1201/9781003466376

Typeset in Caslon
by codeMantra

To our families and friends,
for their encouragement, support, and love.
and
To the dedicated educators globally, who nurture,
guide, support, and ignite a passion for knowledge
and learning in children of every educational background.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Contents

LIST OF FIGURES xv
LIST OF TABLES xvii
FOREWORD xix
PREFACE xxi
ACKNOWLEDGMENTS xxiii
AUTHORS xxiv

CHAPTER 1 CHARACTER EDUCATION AND EMBRACING LEADERSHIP 1
Introduction 1
Character Education — A Quick Review 1
  Importance of Character Education 1
  Defining Good Character 2
  Defining Character Education 2
  Importance of Character Development in Individuals 3
  Building Good Character for Cyber Safety 5
Defining Leadership 6
  What Is Leadership Development? 7
  The Attributes of a Good Leader 7
  Discussing Leadership with Seventh- and Eighth-Grade Students 8
Teaching Leadership Skills to Students in Seventh and Eighth Grade 10
  Creating Student Leadership Opportunities 12
  Engaging Middle School Students in Leadership Roles 13
A Global Social Context and the Development of Leadership Attitude 15
Technology and Leadership — Preparing Students for Their Future 17
  Technology's Enhancements to Leadership Capabilities 17
  Technology's Challenges and Considerations 18
  Teaching Leadership, Cyber Safety, and Embracing Technology 19
Leadership and Fostering Cyber-Safe Behavior 20
  Advancing Online Cyber-Secure Behavior 22
Leadership and Good Character 22
Ethics: A General Introduction and Overview 23
  Defining Values 23

  Defining Morals 23
  Defining Judgment 24
  Defining Norms 24
  Defining Ethical Standards 25
Ethics, Trust, and Cyber Safety 27
  Mutualistic Relationship between Ethics, Trust, and Cyber Safety — Examples 27
Ethics and Leadership 28
  Mutualistic Relationship between Ethics and Leadership — Examples 28
  Ethical Leadership 29
  Teaching Ethical Leadership to Middle School Students 30
  Classroom Discussion on Ethical Leadership — An Approach 30
Ethical Principles for Seventh- and Eighth-Grade Students 32
  Top Five Skills for Cyber Safety in the Mid-21st Century 33
  Leadership in a Digital Age 34
  Ethics in a Digitally Connected World 34
  Maintaining a Proactive Position on Cyber Safety 34
Who Is Generation Alpha? 35
Behavior — What Is Acceptable/Unacceptable? 35
  Anti-Bullying 35
Using Good Judgment by Making Good Decisions 46
Peer Pressure 47
  Influence 47
Susceptibility 47
What Is Good Judgment? 48
  Choices — Where to Start? 49
  Does Gen Alpha Make Decisions Differently than Prior Generations? 49
Artificial Intelligence 54
  What Is Artificial Intelligence? 54
  What Is Generative AI? 55
The Growing Role of Generative AI in Education 56
The Impact of AI on Middle School Students and Academics 58
  The Role of AI in Everyday Life 58
  AI in the Classroom: Enhancing Learning Experiences 58
  AI Beyond the Classroom: Preparing Students for the Future 59
  AI Challenges and Considerations for Educators 59
  Responsible AI (RAI) 60
  Responsible AI and Tech Justice 60
  The Role of Leadership, Maturing AI, and Cyber Safety 62
  Teaching Seventh- and Eighth-Grade Students the Value and Importance of Responsible AI 62
An Overview of AI Fundamentals 63
How Do AI Systems "Learn?" 64
  Training AI Systems 65
  A Step-by-Step Approach to Training AI 66
  Training AI By Example 68
AI Risks: Praemonitus, Praemunitus! 69
  AI Hallucinations 70
  Unethical Uses of AI 70
  The Ethical Use of AI 72
  The Ethical Use of AI: Classroom Discussion and Exercise 73
  Activity: AI Ethics Role-Play 75

High-Level Machine Intelligence (HLMI) 75
genAI Literacy: An Important Goal for Surviving Our Collective Future 76
genAI Literacy: A Foundation 77
genAI Literacy: An Educational Process 79
AI Literacy for Educators 80
One-Year Education Plan of Study: AI Literacy for Educators 83
Quarter 1: Introduction to AI and Its Applications 83
Quarter 2: Understanding AI Tools and Basic Programming 84
Quarter 3: AI in Education and Pedagogy 84
Quarter 4: Advanced AI Concepts and Capstone Project 85
Using AI vs. Abusing AI 86
Summary 87
Chapter 1: Lesson Plans 89
Grade 7 90
Grade 8 130
Notes 174

CHAPTER 2 TECHNOLOGY AND CYBER SAFETY: TEACHING TOMORROW'S DIGITAL CITIZENS 178
Introduction 178
Transitioning from Monitoring to Teaching 178
Cyber Smart: Empowering Student Digital Citizens 179
Online Privacy and Personal Data Protection 179
Oversharing 179
Recommendations — Achieving Online Privacy and Personal Data Protection 180
Maintaining Online Privacy and Protecting Personal Data: A Student Quiz 183
Cyberbullying Awareness and Prevention 184
Social Media and Networking Practices 184
Social Media or Social Networking? 184
Social Media 185
Social Media: Is It Safe Out There? 185
Healthy vs. Unhealthy Social Media 186
Social Media's Impact — Good and Not-so-Good 186
Do You Know Kik? 188
Safer Social Media for Students: Recommendations 188
Social Networking 192
Be Self-Aware: Mitigate Potential Social Networking Risks 193
Parental Controls and Open Dialogue: Creating a Balanced Approach to Online Safety 193
So … How Do I Start That Conversation? 194
Downloading Apps without Permission 195
Additional Protective Measures for a more Cyber-Safe Online Experience 195
Be Proactive, Be Cyber-Safe 197
Password Security and Account Protection 197
Use Strong Passwords or Even Stronger Passphrases 198
Enable Two-Factor Authentication 198
Recommendations for Implementing Two-Factor Authentication 199
Recognizing and Avoiding Phishing Scams 200
Phishing Scams: 10 Red Flags 201
The Darker Side of Phishing Scams 203
Pig Butchering Scam 204

  How Do You Butcher a Pig? 205
  A Scenario Designed for Student Discussion and Engagement 207
  Educator Takeaways from the Scenario Activity 208
  Stay Cyber-Safe: Don't Take the Bait 208
Understanding Digital Footprints 210
  Monitoring Your Cyber Footprint 211
  Managing One's Digital Footprint 211
Fake News and Media/Information Literacy 213
  Exactly What Is Fake News? 213
  SIFT (The Four Moves): Sorting Truth from Fiction 213
  Identifying Hoaxes, Fake News, and Rumors in Social Media 216
  Fake News and Misinformation 216
The Power of AI in Fake News: The Role of Deepfakes 217
  How Are Deepfakes Used? 219
  Mitigating Deepfake Risks 220
  What Is Media Literacy? 221
  Reaching and Teaching Students about Media/Information Literacy 222
The Impact of Screen Time 222
  Defining Screen Time 223
  How Much Time Is Too Much? 225
  Recommendations for Monitoring and Managing "Screen Time" 226
Ethical Use of Technology 227
Risks of Digital Social Networking: Inappropriate Content 228
  Sexting and Sextortion 228
  Global Legislative Overwatch: Sexting and the Law 229
  Sexting: Students at Risk 232
  Online Enticement 233
  Topics for Classroom Discussion 233
Digital Literacy 233
Basic Cybersecurity Awareness 234
Scattered Spider and The Com 234
  Basic Cybersecurity Awareness Recommendations 235
Emerging Technologies — A Look Ahead 237
Summary 238
Chapter 2: Lesson Plans 239
  Grade 7 240
  Grade 8 249
Notes 255

CHAPTER 3 STRANGERS: SAFE/UNSAFE PEOPLE AND THE TRICKY PERSON 260
Why Someone Known Isn't Always Safe 260
  Who Is a Tricky Person? 260
  Who Is and Is Not a Tricky or Unsafe Person? 261
  Additional Interests to Address 261
  Gaming and Avatars — What's Safe, What's Not 263
  What You Post 263
  Why Do Young People Go Online? 267
  Other Ways Apps Can Compromise Young Users 267
  Mandatory Reporters 268
Online Use — Teen Well-Being and Mental Health 269
  An Additional Level of Safety — A Safe-Word 271
Summary 272

Chapter 3: Lesson Plans 273
  Grade 7 274
  Grade 8 282
Notes 291

CHAPTER 4 FROM AWARENESS TO ACTION: INSPIRING STEWARDSHIP IN A DIGITAL AGE 293
Introduction 293
Stewardship 293
Generation Alpha: Pioneers of Environmental Stewardship 295
  How Do We Foster Stewardship Among Teens? 295
  Technological and Data Stewardship — Issues for Student Discussion 297
Cyber Stewardship 299
  What Does It Mean to Be a "Steward of Cyberspace"? 299
  What Makes a Cyber Steward? 299
Cyber Stewardship: Practical Application for the Classroom 300
  #1 Stewardship Discussion Questions (Small Break-Out Groups for Discussion) 300
  #2 Common Cyber Issues Students May Encounter 301
  #3 Cyber Steward Action Plan 301
  #4 My Digital Footprint and the Planet 302
  #5 Create a Cyber Stewardship Pledge 303
Digital Literacy 303
  Empowering Middle School Students through Digital Literacy 305
What Is Digital Citizenship? 305
Frameworks for Digital Citizenship 307
  Choi's Four Categories of Digital Citizenship 307
  Implications for Education and the Educator 308
  Ribble's Nine Elements of Digital Citizenship 309
Empowering Students through Digital Citizenship: A Fusion of Ribble's and Choi's Frameworks 309
  Comprehensive Framework for Digital Behavior 310
  Ethical and Safe Use of Technology 311
  Promoting Critical Thinking and Active Participation 311
  Development of Responsible Digital Habits 311
  Empowering Students to Use Their Voices for Good 312
  Making Digital Citizenship Relevant to 21st-Century Students 312
Practical Application: Digital Citizenship Education in the Classroom 312
Walk in Their Shoes: Online Respect and Perspective-Taking 313
From Cyber Stewardship to Digital Citizenship: Fostering Online Responsibility 314
Ethics, Leadership, and the Responsible Use of Technology 315
  What Are the Traits of Effective Digital Leaders? 315
  How Are Students Able to Demonstrate Leadership Skills in Online Communities? 316
  What Is the Importance of Collaboration in Leadership? 317
  The Ethical Implications of Technology Use 317
  How Does Being a Good Digital Citizen Reflect Respecting Others' Privacy and Digital Rights? 318
  How Can Students Use Technology for Collaborative Problem-Solving and Demonstrate Leadership Qualities? 318
  Discuss Intellectual Property, Plagiarism, and Fair Use 318
  What Does Stewardship Mean to the Teacher's Role? 319
  Stewardship of Students 319

- Stewardship of Influence 319
- Steward of Relationships 320
- Discussion Activity 321
- Earth Day — Smart Practices 322
- Stewardship, Security, and Cyberspace 324
- Can Cyber Safety and Cyber Stewardship Coexist? 325
  - Collaboration #1: Setting Rules for Online Behavior 325
  - Collaboration #2: Protecting Privacy and Data 326
  - Collaboration #3: Stop Cyberbullying 326
  - Collaboration #4: Providing Education and Awareness 326
  - Collaboration #5: Mitigating Hacking and Cyber Threats 326
- Empowering Youth: Addressing Social Issues through Technology 327
- What Is Environmental Stewardship in a Digital Age? 328
- Conclusion 328
- Stewardship Word Find Puzzle 331
- Stewardship Word Find Solution 332
- Chapter 4: Lesson Plans 333
  - Grades 7 and 8 334
  - Grade 7 336
  - Grade 8 342
- Notes 348

EPILOGUE 350

APPENDIX A: TEACHER'S RESOURCE LIST 351

APPENDIX B: RECOMMENDED READINGS 366

APPENDIX C: SOCIAL MEDIA/NETWORKING: ADDITIONAL INFORMATION FOR EDUCATORS AND PARENTS 373

APPENDIX D: DIGITAL BADGES AND CERTIFICATES 386

APPENDIX E: AI FRAMEWORKS 392

APPENDIX F: HIDDEN DANGERS: IDENTIFYING RISKY APPS ON YOUR CHILD'S DEVICE 398

APPENDIX G: THE ANATOMY OF CYBERSECURITY ATTACKS IN THE CONSUMER SPACE 406

APPENDIX H: CYBER SAFETY AND THE ONLINE WORLD: SAFE/UNSAFE PEOPLE & THE TRICKY PERSON: MENTAL WELLNESS STRATEGIES FOR GRADES 7 & 8 428

APPENDIX I: ONLINE USE — TEEN WELL-BEING AND MENTAL HEALTH 434

GLOSSARY OF TERMS & DEFINITIONS 440

INDEX 469

List of Figures

Figure 1.1 Center for creative leadership — DCA leadership model. 7
Figure 1.2 Core principles of ethics. 26
Figure 1.3 Dr. Lo Iacono's eight traits of ethical leadership. 30
Figure 1.4 GAO report — hostile behaviors in K—12 public schools. 36
Figure 1.5 Hate generated bullying. 37
Figure 1.6 Cyberbullying risks. 39
Figure 1.7 Teasing words. 44
Figure 1.8 Stop bullying. 46
Figure 1.9 Daniels fund ethics initiative. 52
Figure 1.10 AI usage in education: four tenets. 60
Figure 1.11 The relationship between AI, NLP, ML, DL, and ANNs. 64
Figure 1.12 AI functional overview. 66
Figure 1.13 Training AI. 67
Figure 1.14 Risks of unethical AI. 71
Figure 1.15 Benefits of ethical AI use. 73
Figure 1.16 The overall impact of achieving HLMI on humanity. 76
Figure 1.17 Foundation of genAI literacy. 78
Figure 2.1 Privacy via two-factor authentication (2FA). 199
Figure 2.2 Example phishing email. 202
Figure 2.3 Example blackmail email. 203

Figure 2.4 Steps in conducting a "Pig Butchering" scam. 206

Figure 2.5 SIFT framework. 214

Figure 2.6 Example of a fake news post on Instagram. 215

Figure 2.7 Youth use screens more as they get older. 223

Figure 2.8 Average daily screen use by gender. 224

Figure 2.9 Average daily screen time. American teens (13- to 18-year-olds). 225

Figure 2.10 Downside of being online. 226

Figure 3.1 Who is behind the screen? 260

Figure 3.2 Mystery person. 265

Figure 3.3 NCMEC sextortion data by month. 267

Figure 4.1 Eight types of stewardship. 294

Figure 4.2 Key components of digital learning. 304

Figure 4.3 Choi's four categories of digital citizenship. 307

Figure 4.4 Planet Earth — environmental sustainability. 322

Figure 4.5 Stewardship word find puzzle. 331

Figure 4.6 Stewardship word find puzzle — solution. 332

Figure G.1 JustDeleteMe website. 409

Figure G.2 Breachsense — data breaches, September 2024. 410

Figure G.3 User screenshot HaveIBeenPwned. 411

Figure G.4 Scattered secrets website. 411

Figure G.5 Scattered secrets compromised passwords. 412

Figure G.6 Gmail flags an email failing its domain's authentication requirements. 419

Figure G.7 ProtonMail flags a suspicious email as a phishing attempt. 419

Figure G.8 Accessing email headers in Gmail. 420

Figure G.9 Accessing email headers in ProtonMail. 420

Figure G.10 Viewing email headers in ProtonMail. 421

Figure G.11 ProtonMail showing the passed DMARC, SPF, and DKIM checks. 422

Figure G.12 ProtonMail showing the failed DMARC, SPF, and DKIM checks. 422

Figure G.13 Gmail showing the passed DMARC, SPF, and DKIM checks. 423

Figure G.14 Gmail showing missing DMARC and DKIM checks. 423

Figure I.1 Teacher's guide to asking about suicide. 436

List of Tables

Table 1.1 The Link between Good Character Traits and Cyber-Safe Habits 6

Table 1.2 Leadership Opportunity Tasks for Middle School Students 12

Table 1.3 Examples of Common AI Usage 55

Table 1.4 Top Generative AI tools 57

Table 1.5 AI Literacy Programs for Educators 82

Table 1.6 Using vs. Abusing AI 87

Table LP 1.7 Nine Bullying Types 107

Table 2.1 Social Media vs. Social Networking 185

Table 2.2 Healthy Social Media vs. Unhealthy Social Networking 187

Table 2.3 Risks Associated with the Kik App 189

Table 2.4 Apps That Can Identify the Location of a Photo 190

Table 2.5 Ways for Students to Mitigate Social Networking Risks 193

Table 2.6 App Monitoring Tools 196

Table 2.7 Managing Your Digital Footprint 212

Table 2.8 Types of Disinformation 218

Table 2.9 Deepfake Usage 219

Table 2.10 Cybersecurity — Global Information Resources 236

Table 4.1 Stewardship Types 294

Table 4.2 Key Issues Related to Technological and Data Stewardship 298

Table 4.3 Ribbie's Nine Elements of Digital Citizenship 309

Table 4.4 Websites That Restrict Harmful or Inappropriate Content 325

Table 4.5 Social Issues and How They Can Be Addressed through Technology 327

Table I.1 The Suicide Lady Podcast, Episodes 2 and 3 437

Foreword

I can attest to the importance of educators being able to recognize when a student is struggling, particularly in relation to their online experiences. Teachers play a critical role—not by becoming technologists or counselors, or expecting students to open up about everything, but by being vigilant, supportive, and responsive. You have the power to notice the subtle changes in behavior that often signal something deeper is wrong.

Do you remember what it was like to be a 13- or 14-year-old? That was a scary enough time trying to figure out who you are, gain independence, and make good decisions. Kids the same age today not only have to worry about those same things, but they are navigating both in a physical world and in a digital world. Suddenly, strangers in vans offering candy isn't the biggest threat! Catfishing, sextortion, deepfakes, digital bullying, and artificial intelligence are all landmines our children must navigate as well.

From Street-smart to Web-wise® provides you with the essential tools to understand today's online world and identify when a student's cyber interactions may be causing emotional or physical harm. More importantly, it empowers you to act appropriately, without judgment, and guide students to the resources they need—helping to prevent their situation from spiraling into a crisis.

The authors of this guide are uniquely qualified to help us navigate this landscape. Al Marcella, Ph.D., CISA, with his extensive experience in IT security and risk management, Brian Moore, with over 20 years in elementary education, and Madeline Parisi, with wide-ranging content development and instructional design experience, combine their expertise to create a resource that not only covers the technical aspects of cyber safety but also addresses the emotional well-being of students. Their deep understanding of both education and technology allows them to provide actionable strategies that are both comprehensive and practical for today's classrooms.

As educators, your role is not to bear the burden of counseling students but to foster an environment where students feel supported, and where you have the tools and knowledge to intervene effectively when necessary. This manual will equip you to do just that—help students navigate their online world safely while ensuring they have the support they need to thrive emotionally.

- Rikki Turner, Ed.D.,

Keynote Speaker, Trainer, and Founder of Still You Rise, Inc., Arizona

Preface

The authors developed this text for teachers and student leaders as the reader and user, and not the student who is the ultimate beneficiary of the material.

This teaching manual is designed to help make an educator's job and knowledge transfer easier by providing context to young learners and by providing relevant lesson plans for each chapter.

The approach is structured to emphasize the following:

- The creation of content in lesson plan format
- The emphasis on skills training and associated assessments
- The development of critical thinking skills regarding cyber hygiene which begins at the earliest ages
- The design and development of instructional materials that can be delivered regardless of the instructor or facilitator's experience level.

In a school classroom environment, it's often best to use inclusive and neutral language when referring to children and educators, as this promotes a respectful and supportive atmosphere.

The reader will notice throughout this book, that instead of using terms such as "girl, boy, he, she, boys, or girls" or using gender-specific terms, the authors will refer to children when discussing pedagogy as "students," "learners," or "young learners." These learners may be involved in any academic learning program, within any positive learning environment serving students.

When referring to teachers, the authors recognize that this descriptor is intentionally broad. The authors use the term teacher or educator to collectively include instructress or instructor, lecturer, tutor, facilitator, mentor, counselor, educationalist, and trainer — i.e., a person who regularly works with children.

Disclaimer

The authors and contributors are not mental health or medical professionals, and any reference to well-being or mental health material is presented to teachers as helpful information and to create awareness of the cues students may display when experiencing well-being trials. It offers suggestions for action. The concepts and responses are designed to make you a trusted person to the students, someone who cares about them, and to whom they can turn when in need and should not be interpreted as professional mental health or medical advice. The information is not a substitute for the qualified knowledge, skills, and judgment of a mental health professional. Always seek immediate mental health or medical professionals when in doubt or when a threat seems imminent.

Examples Are Not Endorsements

This document contains references to materials that are provided for the reader's convenience. The inclusion of these references is not intended to reflect their importance, nor is it intended to endorse any views expressed, or products or services offered by third-party providers. These reference materials may contain the views and recommendations of various subject matter experts as well as hypertext links, contact addresses, and websites to information created and maintained by other public and private organizations.

The opinions expressed in any of these third-party materials included as references or examples do not necessarily reflect the positions or policies of the authors.

The authors do not control or guarantee the accuracy, relevance, timeliness, update, or completeness of any outside, third-party information included in this publication. These references should not be construed as an endorsement by the authors or by the Publisher. The reader should validate and substantiate any information directly from third-party providers before authorizing the acquisition, implementation, or use of any product or service referenced in this book.

Acknowledgments

The authors wish to thank the many contributors who have provided input to this program as it transformed from a concept with various delivery methods to this resource for teachers and those persons who regularly work with children, we thank you.

The authors wish to recognize and thank the following persons for their contributions and for graciously responding to requests for further information:

John F. Boyce, Head-People Development, AMSOIL Inc., Duluth, Minnesota and Adjunct Faculty, Northwestern University, Evanston, Illinois, for providing insight into book development at the earliest stages of transferring the concept to a teacher's manual.

Christine Burke, Elementary School Principal, St. Louis, Missouri, for providing feedback to CRC Press which provided insight to the authors.

Claire Karakey, Licensed Professional Counselor, Clinical Director & Co-Founder, Claibourne Counseling, Scottsdale, Arizona, for providing feedback and resources which helped contribute to content development.

The authors wish to thank the following individuals for their contribution to this book:

Mathias Conradt — Appendix G
Stephanie Nilsen — Appendix H
Mandy Schumacker — Appendix H
Rikki Turner — Appendix I

The authors also thank the anonymous reviewers identified by the Publisher, CRC Press, who initially reviewed our proposed book series and provided positive feedback and comments on the proposed content when the authors initially brought the idea for this book to CRC Press.

Authors

Dr. Al Marcella, Ph.D., CISA, CISM, President of Business Automation Consultants (BAC) LLC, is an internationally recognized public speaker, researcher, IT consultant, and workshop and seminar leader with 46 years of experience in IT audit, risk management, IT security, and assessing internal controls, having authored numerous articles and 30 books on various IT, audit, and security related subjects. Dr. Marcella's clients include organizations in financial services, IT, banking, petrol-chemical, transportation, services industry, public utilities, telecommunications, and departments of government and nonprofits. Dr. Marcella is also a tenured, full-time professor at Webster University, teaching at the Walker School of Business.

Research conducted by Dr. Marcella on unmanned aircraft systems, cyber extortion, workplace violence, personal privacy, electronic stored information, privacy risk, cyber forensics, disaster and incident management planning, the Internet of Things, ethics, and astrophotography has been published in the *ISACA Journal, Disaster Recovery Journal, Journal of Forensic & Investigative Accounting*, *EDPACS*, *ISSA Journal*, *Continuity Insights*, *Internal Auditor Magazine* and the Astronomical League's *Reflector Magazine*. Dr. Marcella's fourth book on cyber forensics, *Cyber Forensics: Examining Emerging and Hybrid Technologies*, a collaborative effort written with a team of six co-authors, was published by CRC Press in 2021.

Dr. Marcella holds a B.S. degree in Management, a B.S. degree in Information Technology Management, an M.B.A. with a concentration in Finance, and a Ph.D. in Management/Information Technology Management. Dr. Marcella is a Certified Information Systems Auditor (CISA), and a Certified Information Security Manager (CISM), and holds an ISACA Cybersecurity Certificate.

Dr. Marcella is the 2016 recipient of the Information Systems Security Association's Security Professional of the Year award and recipient of the Institute of Internal

Auditors Leon R. Radde Educator of the Year 2000 award and has been recognized by the Institute of Internal Auditors as a Distinguished Adjunct Faculty Member. Dr. Marcella has taught IT audit seminar courses for the Institute of Internal Auditors (IIA) and the Information Systems Audit and Control Association (ISACA).

Brian Moore is a passionate Certified K-8 General Education Teacher with over 20 years of experience developing and implementing diverse curriculums covering a wide range of subjects. Moore is highly skilled at motivating students through positive encouragement and reinforcement of concepts via interactive classroom instruction and observation. Moore is successful in helping students develop strong literacy, numeracy, social and learning skills.

Moore has valuable experience in classroom administration, professional development, and project planning in one of Phoenix Arizona's largest Unified School Districts. Prior to the classroom, Moore was the site director for the Scottsdale/Paradise Valley (AZ) YMCA's Before and After School Program.

Equipped with extensive background in versatile education environments, a student-centric instructor, academic facilitator and motivational coach, Moore is well-versed in classroom and online technologies.

Moore received both his Bachelor of Arts and Master of Education: Educational Leadership from Northern Arizona University - Flagstaff, Arizona, and holds Certifications: Standard Professional Elementary Education, K-8 and Pre-K-12 Principal, and the Endorsement: Structured English Instruction, K-12.

Madeline Parisi, M.Ad.Ed., Principal, founded Madeline Parisi & Associates LLC (MPA) in 2013, an international organization providing business training content and training material, after a distinguished career working with professional associations. Together with a pool of subject matter experts, MPA provides business training materials, in-house and virtual training, white-label writing services, and professional certification training and certification exam question development services.

Parisi is a recognized adult education content developer with a 30-plus year career in business training and professional development serving finance, legal, and IT audit, IT security, and risk management professionals.

Parisi holds a Bachelor of Arts degree in Criminology from the University of Illinois, Chicago and a Master of Adult Education from National Louis University, Wheeling, Illinois. Parisi also holds certificates in Volunteer Management from Harper College, Palatine, Illinois and additional certificates in Organizational Development, Lean Six Sigma, and Project Management. Parisi is the author of several columns and articles published in various trade publications and along with Al Marcella, is the co-author of the white paper "Assessing, Managing and Mitigating Workplace Violence: Active Shooter Threat."

Partnering with Al Marcella, The Training Resource Center, LLC, is a jointly operated entity providing training and consulting services, specializing in Environment, Social, and Governance (ESG).

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

1

CHARACTER EDUCATION AND EMBRACING LEADERSHIP

Introduction

> "The quality of a leader is reflected in the standards they set for themselves."
>
> — *Ray Kroc*

We are moving away from focusing on teaching the foundations of good character to teaching what it means to be a leader and developing leadership skills.

In the first three books in the *From Street-smart to Web-wise®: A Cyber Safety Training Program Built for Teachers and Designed for Children* series, Chapter 1 emphasized the importance of teaching good character. In Book 4 as the student matures to a young adult, teaching good behavior is still relevant and important.

However, equally important now is focusing the student's attention beyond the qualities and characteristics that exemplify good behavior to identifying, modeling, and embracing the qualities of being a good and effective leader. Understanding the role that leadership plays in establishing and maintaining a cyber-safe life both for one's self and for others, in a not-so-safe digital world, is an important skill.

As seventh- and eighth-grade students mature into the early stages of adulthood, good character skills learned at an earlier age, now combined with learning leadership skills, will provide students with a solid foundation for successful and productive lives.

Character Education — A Quick Review

Character education plays a crucial role in the holistic development of students, especially those in the seventh and eighth grades. It is as essential as physical activities and academic assignments, contributing significantly to their maturation into responsible adults. By teaching honesty, kindness, and good friendship, students are equipped with the necessary tools to act responsibly, care for others, and navigate life's challenges effectively.

Importance of Character Education

Character education creates a positive and inclusive learning environment that fosters a sense of belonging and emotional well-being among students. When introduced

DOI: 10.1201/9781003466376-1

early in academic life, it helps students develop essential social skills, improve classroom behavior, and enhance their ability to communicate and collaborate effectively. This holistic approach molds students into well-adjusted individuals who can positively impact their communities and society at large. Empowering students to make ethical decisions, resolve conflicts amicably, and navigate challenges is crucial in their evolving educational journey and in the world around them.

Defining Good Character

Good character consists of habitual positive qualities manifested in thoughts, emotions, and behaviors that benefit both individuals and society. It is developed through consistent practice and adherence to ethical values. Qualities such as perseverance, love of learning, and prudence significantly impact school success and student satisfaction, as well as positive classroom behavior. According to a study by Marco Weber et al., good character is relevant for both subjective (e.g., satisfaction) and objective (e.g., grades) outcomes in school settings.[1]

To possess good character, one must know the good, act in morally good ways, and be inclined toward the good through the development of virtues. Virtue, particularly prudence (knowing what to seek and what to avoid), is integral to forming good character and ensuring the person's integrity.

Defining Character Education

Character education is the deliberate effort to foster positive qualities and values in individuals to develop good character traits. It goes beyond academic instruction, focusing on instilling virtues, ethical principles, and social skills that contribute to personal and social well-being. Character education aims to shape individuals into responsible, respectful, and compassionate members of society.

Key components of character education are as follows:

- Values and Virtues: Emphasizing core values like honesty, integrity, responsibility, fairness, respect, and empathy.
- Ethical Decision-Making: Providing tools and skills for making ethical decisions, involving critical thinking and problem-solving.
- Social and Emotional Learning: Helping individuals manage emotions, develop empathy, and build positive relationships.
- Civic and Global Responsibility: Encouraging responsibility toward the community and the larger world, promoting civic engagement and social justice.
- Resilience and Perseverance: Teaching coping mechanisms for challenges, fostering resilience and perseverance.
- Positive Behavior Reinforcement: Recognizing and reinforcing positive behaviors to create a supportive learning environment.

- Role Modeling: Demonstrating positive character traits through the actions and behavior of influential figures.
- Community Involvement: Engaging in activities that promote community service and collaboration.

Character education is often integrated into formal educational curricula and can be implemented in schools, families, and community organizations. The goal is to develop individuals who excel academically and contribute positively to society through their character and ethical conduct.

Importance of Character Development in Individuals

Character education actively prepares students for modern life's challenges. It provides balance to media and Internet messages. As other influences decline, schools actively offer stable community values. Character education principles are traditional yet actively equip students for the future by providing core values with academics to develop responsible citizens.

While academically correct, how does one explain the "what" of character development in terms that young, maturing middle school students will understand? Well, one does so by transferring the principles of character development into meaningful examples that these students can relate to.

The concept of character education in the seventh and eighth grades is more easily understood by students when discussed in age-appropriate terms and with age-appropriate examples.

The following provides a stepwise process that an educator[I] may wish to use to assist seventh- and eighth-grade middle school students in understanding and internalizing the principles of character education through relatable examples and practical activities.

Teaching Tip

Step 1: Introduction to Character Education

- Objective: Introduce the concept of character education and its importance.
- Activity: Start with a class discussion asking students what they think "character" means.
- Example: Explain that character education is about learning to be a good person by being honest, kind, respectful, and responsible.

[I] This chapter refer to "educators" and that language is intended to be inclusive of all school personnel that may impact teaching and learning like classroom teachers, university professors, instructors, lecturers, paraprofessionals, guidance counselors, mentors, trainers, coaches, tutors, and administrators.

Step 2: Defining Core Values

- Objective: Identify and explain core values associated with good character.
- Activity: Create a list of core values such as respect, responsibility, fairness, and kindness.
- Example: Use relatable scenarios like sharing with a friend (kindness) or admitting a mistake (honesty).

Step 3: Relating Values to Everyday Life

- Objective: Show how core values apply to students' daily lives.
- Activity: Discuss real-life examples and ask students to share their own experiences.
- Example: Talk about helping a new student feel welcome (respect) or following through on a promise to help with a group project (responsibility).

Step 4: Role-Playing Activities

- Objective: Practice character values through role-playing.
- Activity: Divide students into groups and assign scenarios to act out, demonstrating core values.
- Example: Role-play a situation where a student finds money on the ground and decides to give it to a teacher (honesty).

Step 5: Discussing Media and Internet Influence

- Objective: Address how media and the Internet can impact character.
- Activity: Analyze examples from social media, TV shows, or movies where characters display good or bad behavior.
- Example: Discuss a popular TV show where a character stands up for a friend being bullied online (courage and kindness).

Step 6: Creating a Class Student Credo

- Objective: Develop a class agreement on how to treat each other based on core values.
- Activity: Collaboratively create a class credo that outlines how students will embody these values.
- Example: A starting point for a student Credo, which may be modified based on your student's objectives and goals, would read as such…

Student's Good Character Credo

We, the students, pledge to uphold the pillars of good character:

- Caring: We commit to kindness in all our interactions.
- Citizenship: We promise to contribute positively to our community.
- Compassion & Empathy: We strive to understand and share the feelings of others.
- Fairness: We vow to treat all people equitably and justly.
- Honesty & Integrity: We pledge to act truthfully and honorably.
- Loyalty: We promise steadfast allegiance to our values and peers.
- Parental Influence & Family Role: We acknowledge and respect the guiding influence of our families in shaping our principles.

- Perseverance: We are determined to overcome challenges with resilience.
- Respect: We will show esteem and regard for all.
- Responsibility: We accept accountability for our actions.
- Trustworthiness: We commit to being reliable and dependable in all our duties.

Through these values, we define our path to character excellence.

Step 7: Reflecting on Personal Growth

- Objective: Encourage self-reflection on personal character development.
- Activity: Have students keep a journal where they write about times they demonstrated good character or faced challenges in doing so.
- Example: Prompt students to reflect on a time they apologized for a mistake and how it made them feel (self-awareness and growth).

Step 8: Recognizing and Celebrating Character

- Objective: Reinforce positive behavior by acknowledging good character.
- Activity: Create a "Character Wall," where students can post notes recognizing their peers' positive actions.
- Example: A student writes, "I saw Emily helping John with his homework even though she was busy," and posts it on the wall.

Step 9: Ongoing Conversations and Support

- Objective: Maintain an open dialogue about character development.
- Activity: Regularly check in with students about their experiences and feelings regarding character education.
- Example: Hold weekly discussions where students can share challenges and successes related to living out the core values.

Step 10: Connecting to Broader Community

- Objective: Extend character education beyond the classroom.
- Activity: Organize community service projects or school-wide initiatives that promote core values.
- Example: Plan a clean-up day at a local park to teach responsibility and care for the environment.

Building Good Character for Cyber Safety

Building good character is foundational in shaping behaviors and decision-making, including online activities. Responsibility, respect, integrity, and courage are crucial for fostering cyber-safe habits. When these traits are applied to online activities, they help mitigate common digital risks like oversharing, cyberbullying, and scams. By fostering virtues like responsibility and respect, students learn to protect themselves online and contribute to a healthier digital community.

Educators, parents, and policymakers can develop more effective strategies to promote both character education and cyber safety. Good character is not just an offline asset but a critical component of safe and ethical behavior in the digital age, ensuring that students are well equipped to handle the challenges of both the real and virtual worlds.

Table 1.1 identifies how different aspects of good character contribute to cyber safety and provides examples educators may use to illustrate these points (see Table 1.1).

Table 1.1 The Link between Good Character Traits and Cyber-Safe Habits

GOOD CHARACTER TRAIT	TRAIT DESCRIPTION	CYBER SAFETY EXAMPLE
Responsibility	In the digital context means understanding the impacts of one's actions online and taking accountability for them. This involves using technology in a way that is safe and respects the rights and privacy of others.	A student might think twice before sharing a friend's private message without permission. Recognizing that such an action could betray trust and cause harm, the responsible individual chooses to respect their friend's privacy, thus avoiding potential emotional distress.
Respect	Respect involves acknowledging the rights and feelings of others online, just as one would offline. It includes engaging in courteous communication and valuing others' opinions, even when they differ from one's own.	When participating in online forums or social media discussions, a person with high respect for others will avoid using harsh language or making offensive comments. This not only prevents cyber conflicts but also promotes a positive online community environment.
Integrity	Integrity entails being honest and upstanding in all situations, including the digital world. This means not engaging in or endorsing dishonest behaviors such as spreading false information or using someone's data without consent.	A student avoids clicking on suspicious links or downloading illegal software, regardless of the potential benefits, such as free access to otherwise paid content. This behavior helps mitigate the risk of malware and promotes a safer, more secure digital environment.
Courage	Courage in cyber safety means standing up against wrongdoing and supporting others who might be victims of online abuse. It involves the bravery to report inappropriate behaviors and support efforts to maintain digital ethics.	Seeing a classmate being bullied online, a courageous student might report the behavior to the necessary authorities (like a school counselor or the social media platform) or reach out to support the victim, thus helping to stop the cyberbullying

Defining Leadership

The definition of leadership varies based on who is defining it and whether that individual is an academic or an industry professional.

The Center for Creative Leadership (CCL) views leadership as a social process that enables individuals to work together to achieve results that they could never achieve working as individuals.

The CCL's Direction, Alignment, and Commitment (DAC) model for leadership moves beyond the idea of leaders, followers, and shared goals, with the revolutionary idea that leadership happens when a group of people are producing direction, alignment, and commitment. In other words, the DAC model showcases how leadership happens in the interactions and exchanges among people with shared work.

Regardless of the structure, team, workgroup, task force, department, etc., CCL postulates that the group needs

- agreement about its **direction** and what they are trying to accomplish together,
- **alignment** for effective coordination of the work in service of their shared direction, and
- strong **commitment** to prioritize the success of the collective[2] (see Figure 1.1).

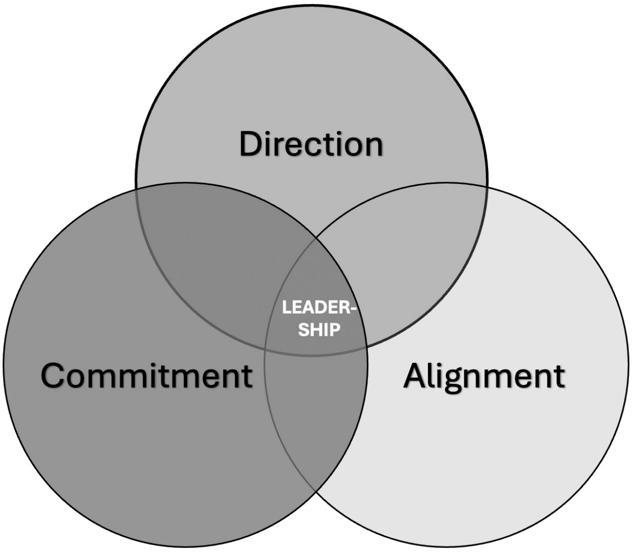


Figure 1.1 Center for creative leadership — DCA leadership model.[3]

For purposes of our discussion here, leadership is defined as the ability to influence, guide, and motivate a group of people toward achieving a common goal or purpose. It involves a social process that enables individuals to work together effectively, leveraging their collective strengths to achieve results that are unattainable when working alone. While leadership can be associated with a person's title, seniority, or ranking within a hierarchy, it fundamentally revolves around the capacity to inspire and direct others in pursuit of shared objectives.

What Is Leadership Development?

Leadership development is the process of enhancing an individual's ability to perform effectively in leadership roles within an organization. It encompasses a set of activities and programs designed to prepare current and future leaders by improving their skills, abilities, and confidence. Leadership development focuses on cultivating broad capabilities, such as self-awareness and resilience, necessary to adapt to dynamic and evolving challenges. It involves fostering alignment with organizational strategy, gaining mindshare, and developing the talents of others, ultimately shaping employees into well-rounded individuals who are the right fit for leadership positions.

The Attributes of a Good Leader

Research conducted by Lavery and Coffey with middle school students suggests that students view leadership qualities or attributes to be broad and almost all-inclusive.

Leaders need to be people of integrity, they must be other-centered and relational in their leadership, they should be courageous, and finally, leaders need to be inspirational. Leaders should be "compassionate toward everyone," generous, kind, and respectful. They need to be empathetic, where they put themselves "in others' shoes" to consider how the choices they make will affect the people they lead. They must have a "good sense of justice," leaders should "make change for the good," do "what's right, not what's easy," "do the right thing," and "be humble and act" so that the world is a better place.

Finally, leaders should not "put themselves first," be brash, overbearing, or "think they're better than everyone." Leaders should "work with their people", and "know their people … each one individually." Leaders should inspire others "by setting an example worth following" and "value others' opinions as well as their own."

Continuing on, students believe that leaders need to be inclusive, and courageous, and must be prepared to enact "what needs to be done, no matter the path or the difficulties in the way." Leaders should be inspirational, i.e., leaders need to "inspire people, inspire others to do things." Students noted that communication requires leaders "to be good listeners, listening to everyone."

The results from the student focus group interviews conducted by Lavery and Coffey indicated that middle school students have very firm views about what leadership is and is not. The participants perceived leadership as process-directed (goal-oriented), relational, and service-oriented.

It was apparent from the responses of the participants to the question "Name someone you consider to be a good leader" that the middle-school students had a more comprehensive view of leadership than someone who might simply be considered a hero.

An understanding of leadership — i.e., distributed, transformational, and servant — sits well with the middle school students' conviction that good leaders are role models for others, hold firm to their beliefs, and make hard decisions when necessary while being empathetic at all times. Hence, leaders are good communicators — both verbal and nonverbal — who can be trusted to do what is in the best interests of everyone.[4]

Discussing Leadership with Seventh- and Eighth-Grade Students

> Leadership experience in middle school is incredibly beneficial for students. It not only helps them build essential life skills but also prepares them for future academic and professional endeavors. Developing leadership skills at a young age can have a profound impact on personal growth and success.[5]

Discussing leadership with seventh- and eighth-grade students is crucial because it lays the foundation for essential life skills that they will carry into adulthood. At this developmental stage, students are beginning to form their identities and are more receptive to understanding and adopting values such as responsibility, integrity, and teamwork. By introducing leadership concepts early, educators can help students develop a sense of self-awareness and confidence that will empower them to take initiative and make positive decisions throughout their lives.

Furthermore, teaching leadership skills helps students improve their interpersonal and communication abilities. Effective leaders must work well with others, listen actively, and articulate their ideas clearly. These skills are not only vital for successful leadership but are also important for academic success and social interactions. By engaging in leadership discussions and activities, students learn how to collaborate, resolve conflicts, and build strong, respectful relationships with their peers and teachers.

Leadership is a fundamental aspect of life, and educational institutions play a crucial role in nurturing future leaders. Middle school students, particularly those in grades 7 and 8, are at a critical developmental stage where leadership skills can be effectively instilled.

Leadership is not just about possessing certain traits but also about developing specific skills through structured programs and activities. These skills include technical abilities, human relations, and conceptual understanding. Middle school students benefit from leadership programs that foster these abilities, enhancing their self-confidence, communication skills, and ability to work effectively in teams.

Discussing leadership encourages students to think critically about their roles within their communities. It helps them understand the impact they can have and motivates them to contribute positively. Whether in school projects, extracurricular activities, or community service, students who grasp the principles of leadership are more likely to step up, take responsibility, and inspire others. This sense of civic duty and community involvement is essential for creating future leaders who are committed to making a difference in their surroundings.

Transformational leadership involves motivating and inspiring followers to achieve higher levels of performance and personal development. In the context of education, teachers who practice transformational leadership can significantly impact their students' academic and social growth. By engaging students in problem-solving and critical-thinking activities, teachers can help them develop the skills and confidence needed to take on leadership roles.

Leadership education fosters resilience and adaptability in students. As they engage in leadership roles and face various challenges, they learn to persevere and adapt to changing circumstances. This builds their capacity to handle stress and overcome obstacles, which is critical in today's fast-paced and ever-evolving world. By discussing and practicing leadership, seventh- and eighth-grade students are better prepared to navigate their educational journeys and future careers with resilience and confidence.

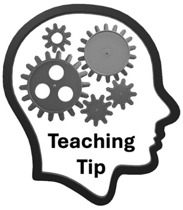
Research conducted by Esther Haynes-Tross suggests that middle school is an ideal time to develop leadership skills in students. By integrating leadership training into the curriculum and fostering a school culture that values leadership, educators can help students build the confidence and skills needed to succeed in future academic and career endeavors. The research findings provide valuable insights for stakeholders looking to enhance leadership development in middle schools, emphasizing the need for a balanced approach that includes both academic and leadership training.[6]

Schools are charged with providing middle school students with the knowledge and skills needed to orient them to high school and beyond and to build future leaders in the global society of this 21st century. By addressing and teaching leadership skills and providing structured opportunities for students to develop their leadership abilities, middle schools can play a pivotal role in shaping the leaders of tomorrow.

Teaching Leadership Skills to Students in Seventh and Eighth Grade

> All middle school students have the leadership skills potential that are eagerly awaiting an opportunity to be developed. It is only through a greater emphasis on this development that we, as a society, can make a marked improvement in our future, our students, and for generations to come.[7]

Educators may wish to consider the five steps outlined here, as a method of effectively introducing the concepts of leadership and leadership development to seventh- and eighth-grade students, assisting them to understand and embody the principles of good leadership.



Step 1: Introduction to Leadership

- Objective: Define leadership and its importance.
- Explanation: Leadership is the ability to guide, influence, or inspire others. A leader is someone who others want to follow, not someone who forces others to follow.
- Activity: Begin with a classroom discussion about what leadership means. Use the definition provided to explain that leadership involves influencing, guiding, and motivating others to achieve a common goal.
- Example: Share examples of famous leaders, such as Malala Yousafzai, Michelle and Barack Obama, Martin Luther King Jr., Rosa Parks, Mother Teresa, Princess Diana, Nelson Mandela, and Winston Churchill, and discuss how these individuals influenced and motivated people.

Step 2: Identifying Personal Leadership Qualities

- Objective: Help students recognize the key qualities/attributes of effective leaders.
- Explanation: Everyone has unique qualities that can make them a good leader, such as being kind, responsible, or good at solving problems.
- Activity #1: Create a list of leadership qualities/attributes with the class (refer to the list discussed earlier in the chapter as a starting point), such as responsibility, communication, empathy, and resilience.
  - Example: Ask students to identify these qualities in characters from popular books or movies, like Katniss Everdeen from “The Hunger Games” or Harry Potter from the “Harry Potter” series.
- Activity #2: Self-Reflection Exercise. Have students list their strengths and think about how these can help them lead.
  - Example: Being good at sports might make them a good team captain.

Step 3: Leadership in Action

- Objective: Illustrate how leadership works in real-life scenarios.
- Explanation: A leader works well with others and values everyone's contributions.
- Activity: Organize role-playing exercises where students take turns being the leader in various situations, such as leading a group project or organizing a class event.
- Example: Set up a scenario where students have to plan a class field trip. The chosen leader must delegate tasks, ensure everyone's ideas are heard, and make decisions based on group input.

Step 4: Developing Leadership Skills

- Objective: Enhance students' leadership abilities through practice.
- Explanation: Leaders take responsibility for their actions and the actions of their team. They also admit when they are wrong and learn from their mistakes.
- Activity: Implement activities that build leadership skills, such as team-building exercises, public speaking opportunities, and problem-solving tasks.
- Example: Hold a debate on a topic relevant to student interests. Assign roles such as moderator, debater, and researcher to encourage different leadership styles and collaboration.

Step 5: Reflecting on Leadership Experiences

- Objective: Encourage self-awareness and resilience.
- Explanation: Leaders often need to make decisions and solve problems. This involves thinking critically and considering different perspectives.
- Activity: Have students reflect on their experiences with leadership, both in and out of the classroom. Use journals or group discussions to share what they learned about themselves and their abilities.
- Example: Ask students to write a short essay on a time they had to lead a group, what challenges they faced, and how they overcame them. Discuss how these experiences will help them become better leaders in the future.

Additional leadership skills that educators should consider discussing with students include…

Communication Skills

- Clear and effective communication is essential for good leadership. This includes listening to others and expressing ideas clearly.
- Example: Role-Playing: Create scenarios where students must lead a group discussion or resolve a conflict. For instance, simulate a situation where they must organize a school event and need to delegate tasks to classmates.

Empathy and Emotional Intelligence

- Good leaders understand and care about the feelings of others. This helps them to inspire and support their team.
- Example: Peer Mentoring: Pair older students with younger ones for a mentoring session. The older students can help with homework or just talk about their day. Discuss the importance of understanding and helping others.

Setting Goals and Planning

- Leaders set goals and create plans to achieve them. This helps keep their team focused and motivated.
- Example: Goal-Setting Workshop: Have students set a personal or group goal, like improving their grades or starting a new club, and create a step-by-step plan to achieve it. Regularly check in on their progress and adjust the plan as needed.

Creating Student Leadership Opportunities

Research conducted by Esther Haynes-Tross, disclosed that students believed strongly that teachers played a significant role in their lives, and the students relied heavily on the teachers daily to develop their leadership skills and academic growth and to show them the way of life.

Additionally, Haynes-Tross's study identified that efforts were made by administrators and teachers to assign as many students as possible to leadership tasks in the school setting to develop their leadership skills. However, the research revealed that not enough tasks are created or available to accommodate the many students who are eager to accept leadership assignments in and out of the classroom environment to develop their leadership skills.[8]

Directly addressing the shortcomings identified by Haynes-Tross, Table 1.2 provides a list of tasks that an educator may assign a student. These tasks are designed to assist the student in gaining valuable leadership experience.

Table 1.2 Leadership Opportunity Tasks for Middle School Students

TASK	LEADERSHIP BENEFIT
Classroom group project leader	Develops organization, delegation skills, and the ability to motivate and manage peers.
Student council representative	Enhances public speaking, decision-making, and understanding of democratic processes and civic engagement.
Peer tutoring	Builds communication skills, empathy, and the ability to teach and support others.
School event organizer	Fosters project management, teamwork, and creativity in planning and executing events.
Classroom helper	Encourages responsibility, reliability, and the ability to assist teachers and classmates effectively.

(*Continued*)

Table 1.2 (*Continued*) Leadership Opportunity Tasks for Middle School Students

TASK	LEADERSHIP BENEFIT
Library volunteer	Develops time management, organizational skills, and a sense of service and community involvement.
Team captain (sports or clubs)	Enhances leadership in a team setting, including motivation, strategy, and sportsmanship.
Environmental club leader	Promotes awareness and action on environmental issues, fostering responsibility and activism.
Technology assistant	Builds technical skills, patience, and the ability to teach and assist others with technology.
Mentoring younger students	Develops mentoring skills, patience, and the ability to guide and support younger peers.
Fundraising organizer	Enhances planning, financial management, and persuasive communication skills.
Safety patrol member	Encourages responsibility, vigilance, and the ability to ensure the safety and well-being of others.
Class discussion leader	Builds confidence in leading discussions, critical thinking, and the ability to facilitate group dialogue.
Homework club leader	Develops organizational skills, responsibility, and the ability to support and motivate peers academically.
Art club coordinator	Fosters creativity, planning, and the ability to coordinate and inspire peers in artistic activities.

Engaging Middle School Students in Leadership Roles

Educators may wish to consider the following activities as additional avenues to engaging and encouraging their students to take on leadership roles and responsibilities.

1. Guiding Class Discussion
   In a classroom setting, middle school students can sharpen both their leadership skills and their public speaking skills by leading a class discussion.
   Application of the Learning Process:
   Have the class read a book of poems; each student might be asked to lead a short class discussion on their favorite poem in the book. As they call on their peers and guide the discussion, even hesitant students will start to discover a sense of newfound confidence in their leadership abilities.
2. Learning in Multiage Classrooms
   Leadership isn't always about being in charge. Sometimes, a good leader is someone who offers help and guidance when it's needed.
   Application of the Learning Process:
   Older students can be assigned to help younger classmates with homework assignments or provide coaching guidance in solving challenging math problems or learning a new skill.
3. Serving the Community
   Leadership and service go hand in hand. When service is part of a child's education from the start, that child will ultimately develop a focus on the needs of others.

Application of the Learning Process:

Have the students identify and design a community service project, cleaning a neighborhood park, for example. Then allow them to implement their community service project.

4. Participation in Team Sports or Activities

Participation in team sports or activities by seventh- and eighth-grade students helps them learn leadership skills in several ways:

- Teamwork: Students learn to work with others, listen, and share responsibilities.
- Communication: They practice giving and receiving feedback and expressing ideas clearly.
- Problem-Solving: They face challenges and must find solutions, often leading others in this process.
- Confidence: Successfully leading a team builds self-esteem and confidence in their abilities.
- Responsibility: They learn to take responsibility for their actions and decisions, which is crucial for leadership.

Application of the Learning Process:

Separate the students into small groups (group size is dependent on the number of students in the class). Each group is given a project to complete within a set time frame. The project could be something like planning a school event, creating a class presentation on a historical topic, or designing a simple science experiment. Each group must choose a team leader to guide the project. Each group member is assigned specific tasks relative to the project selected.

5. Pursuing Personal Projects

Counterintuitive to participation in team sports or activities, when middle schoolers delve into an independent study project or even a hobby, they cultivate confidence and self-efficacy. Both qualities prime them to be leaders.

Application of the Learning Process:

Encourage students to choose a personal interest or hobby and develop it into a project over a semester. This could be anything from writing a short story, creating a piece of art, building a model, conducting a simple science experiment, or starting a small community initiative. The key is that it should be something they are passionate about.

Through this personal passion project, students gain confidence by pursuing and completing something they are deeply interested in. They develop self-efficacy by overcoming challenges and taking responsibility for their learning. The process of planning, executing, and presenting their project helps them develop essential leadership skills that will serve them in various aspects of their lives.[9]

A Global Social Context and the Development of Leadership Attitude

On the global stage, the Organisation for Economic Co-operation and Development (OECD), the United Nations Educational, Scientific and Cultural Organization (UNESCO), and the European Union (EU) have a vested interest in the social context and the development of leadership attitudes because these factors are critical to achieving their broader missions of fostering inclusive and sustainable development.

OECD, UNESCO, and the EU each play significant roles in shaping the social context and developing leadership attitudes through their guidelines and policies.

Overall, the collective interest of these organizations in the social context and leadership development underscores their commitment to preparing future generations to lead with integrity, innovation, and a global perspective.

The Organisation for Economic Co-operation and Development:

OECD is an international organization that aims to promote policies that improve the economic and social well-being of people around the world. It provides a platform for governments to collaborate on key issues such as economic growth, financial stability, education, and environmental sustainability. The OECD's mission is to shape policies that foster prosperity, equality, opportunity, and well-being for all, by conducting research, publishing data and analysis, and facilitating discussions among its member countries.

Influence on Social Context:

The OECD's guidelines, particularly those related to education and skills development, emphasize the importance of equitable and inclusive education systems. By advocating for policies that promote access to quality education for all, the OECD influences the social context by addressing disparities and fostering a culture of lifelong learning. This approach helps create more inclusive societies where individuals are better prepared to participate fully in the economic and social life of their communities.

Effect on Development of Leadership Attitudes:

The OECD's focus on fostering key competencies, such as critical thinking, collaboration, and adaptability, directly impacts the development of leadership attitudes. By promoting educational practices that encourage these skills, the OECD helps shape students into proactive and innovative leaders. Their emphasis on 21st-century skills ensures that future leaders are not only knowledgeable but also equipped to navigate complex challenges and drive positive change in their societies.

The United Nations Educational, Scientific and Cultural Organization:

UNESCO is a specialized agency of the United Nations aimed at promoting peace and security through international cooperation in education, science, culture, and communication. Its purpose is to contribute to the building of peace, the eradication of poverty, sustainable development, and intercultural dialogue by promoting collaboration among nations. UNESCO's mission includes fostering educational opportunities, protecting cultural heritage, advancing scientific research, and ensuring freedom of expression.

Influence on Social Context:

UNESCO's guidelines emphasize the role of education in promoting peace, sustainable development, and intercultural dialogue. By advocating for global citizenship education, UNESCO influences the social context by encouraging students to appreciate cultural diversity and understand global issues. This fosters a more harmonious and interconnected world, where individuals are aware of their responsibilities toward global sustainability and human rights.

Effect on Development of Leadership Attitudes:

UNESCO's guidelines encourage the development of leadership attitudes that are grounded in ethical principles and a commitment to social justice. By promoting education that focuses on human rights, environmental stewardship, and cultural awareness, UNESCO helps cultivate leaders who are not only effective but also compassionate and responsible. These leaders are better prepared to advocate for and implement policies that promote cyber safety, social equity, and environmental sustainability.

European Union:

The EU is a political and economic union of member states located primarily in Europe. Its role is to foster economic cooperation and ensure stability and peace across the continent. The purpose of the EU is to create a single market through standardized laws that apply in all member states, allowing for the free movement of goods, services, people, and capital. The mission of the EU includes promoting economic growth, ensuring environmental sustainability, protecting human rights, and enhancing the quality of life for its citizens through collaborative policies and initiatives.

Influence on Social Context:

The EU's guidelines, particularly those outlined in the European Education Area initiative, aim to create a cohesive educational framework across member states. This harmonization of educational standards and recognition of qualifications fosters mobility and cooperation among European citizens. By promoting inclusivity and reducing educational disparities, the EU influences the social context by enhancing social cohesion and a sense of European identity.

Effect on Development of Leadership Attitudes:

The EU's emphasis on competencies such as multilingualism, digital literacy, and entrepreneurship fosters the development of dynamic and versatile leadership attitudes. By encouraging cross-cultural exchanges and collaboration, the EU helps develop leaders who are open-minded, innovative, and capable of leading in a multicultural environment. These leaders are equipped to drive economic growth and social progress while navigating the complexities of a diverse and interconnected European landscape.

Technology and Leadership — Preparing Students for Their Future

Current and emerging technologies have and will continue to profoundly impact an individual's leadership capabilities, enhancing them in several ways while also presenting new challenges. It is essential that educators proactively address the increasing role of technology in society and prepare students to live and work in an omnipresent digital world.

Technology's Enhancements to Leadership Capabilities

Improved Communication and Collaboration:

- Technologies such as videoconferencing, instant messaging, and collaborative platforms enable leaders to communicate effectively with their teams, regardless of geographical location. This fosters real-time collaboration and decision-making, which is essential for modern leadership.
- Example: A manager using tools like Slack or Microsoft Teams can coordinate with remote team members, ensuring everyone stays informed and engaged.

Access to Information and Data-Driven Decision-Making:

- Leaders now have unprecedented access to data analytics and business intelligence tools that provide insights into market trends, employee performance, and customer behavior. This allows leaders to make informed decisions based on empirical data rather than intuition alone.
- Example: A marketing leader using Google Analytics can track a marketing campaign's performance in real time and adjust strategies accordingly to maximize impact.

Enhanced Productivity and Efficiency:

- Automation and artificial intelligence (AI) can handle routine tasks, allowing leaders to focus on strategic planning and innovation. Tools like AI-driven project management software streamline workflows and ensure that teams remain productive and efficient.
- Example: A project manager using project management software such as Trello or Asana can automate task assignments and deadlines, freeing up time to focus on high-level project strategy and team development.

Global Reach and Diverse Teams:

- Technology allows leaders to build and manage diverse teams from around the world, bringing in varied perspectives and expertise. This diversity can lead to more innovative solutions and a better understanding of global markets.
- Example: A product development leader can leverage videoconferencing and collaborative tools to bring together designers, engineers, and marketers from different countries to create a product that appeals to a global audience.

Technology's Challenges and Considerations

Digital Literacy and Adaptability:

- Leaders must continuously update their digital skills to keep pace with rapidly evolving technologies. Those who fail to adapt may struggle to effectively lead in a tech-driven environment.
- Example: A leader who does not understand the basics of cybersecurity may inadvertently put their organization at risk.

Maintaining Human Connection:

- While technology facilitates communication, it can also create a barrier to genuine human connection. Leaders must find a balance between leveraging technology and maintaining personal interactions to build trust and rapport with their teams.
- Example: A leader might use regular virtual team-building activities to foster a sense of community and connection among remote employees.

Data Privacy and Security:

- The reliance on digital tools and data analytics requires leaders to prioritize data privacy and security. Breaches can undermine trust and have severe legal and financial repercussions.
- Example: A leader must implement robust cybersecurity measures and ensure their team follows best practices to protect sensitive information.

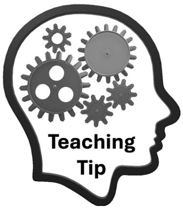
Overreliance on Technology:

- There is a risk of over-relying on technology, leading to diminished problem-solving and critical thinking skills. Leaders need to ensure that technology is used as a tool to enhance, not replace, human judgment.
- Example: A leader should encourage their team to brainstorm and develop creative solutions independently before turning to technology for answers.

Current and emerging technologies significantly enhance leadership capabilities by improving communication, enabling data-driven decisions, increasing productivity, and fostering global collaboration. However, leaders must navigate challenges such as maintaining digital literacy, fostering human connections, ensuring data security, and avoiding overreliance on technology to effectively lead in the digital age.

Teaching Leadership, Cyber Safety, and Embracing Technology

The following represent practical examples that an educator may use to teach seventh- and eighth-grade students about the importance of cyber safety and leadership in the digital age.



1. Maintaining Digital Literacy
   - Example: Explain the importance of keeping software and apps updated to protect against viruses and hackers.
     - Activity: Have students perform a "software update day" where they check and update all their devices and apps. Discuss why these updates are important for security.
2. Fostering Human Connections
   - Example: Discuss how face-to-face interactions and empathy can sometimes be lost in digital communication.
     - Activity: Organize a class debate or discussion where students must argue for and against a topic. Afterward, compare the experience with an online discussion and talk about the differences in communication.
3. Ensuring Data Security and Privacy
   - Example: Use the analogy of a locked diary or one's private email to explain the importance of strong, unique passwords for online accounts.
     - Activity: Conduct a password strength workshop where students create strong passwords using guidelines (e.g., a mix of letters, numbers, and symbols). Explain why these passwords are important for protecting their personal information. Introduce the concept of "passphrases" (A passphrase is a type of password made up of several words instead of just one word or a mix of letters and numbers. It's easier to remember but harder for others to guess because it's longer. For example, "BlueHorseRunsFast!" This passphrase uses four simple words and a punctuation mark to make it strong and secure.
4. Avoiding Online Scams and Threat Actors
   - Example: Share stories of common scams targeting teenagers, such as fake scholarships or online contests.
     - Activity: Have students work in groups to create posters highlighting common online scams and how to avoid them. Display these posters around the school to raise awareness.
5. Learning to Effectively Lead in the Digital Age
   - Example: Explain how digital tools can be used for group projects and organizing events, and enhancing leadership skills.
     - Activity: Assign a group project where students must use collaborative tools (like Google Docs or Trello) to plan and execute a small event or project. Discuss how these tools helped or hindered their leadership and teamwork.

By using these relevant and age-appropriate examples, educators can effectively teach middle school students about the importance of cyber safety and leadership in the digital age, preparing them to navigate the digital world safely and responsibly.

Leadership and Fostering Cyber-Safe Behavior

Educators may elect to engage with seventh- and eighth-grade students discussing steps to become more aware of the importance of cyber safety and protecting themselves and their friends from online threats by addressing the following connections between leadership and cyber safety practices.

1. Responsibility and Accountability: Leaders learn to take responsibility for their actions. This helps in being careful online and understanding that their actions have consequences.
   Example: A class president makes sure their school's social media accounts use strong, unique passwords and encourages classmates not to share passwords with others.
2. Strategic Thinking and Risk Management: Leaders think ahead and plan for potential problems. This helps in identifying online risks and figuring out how to avoid them.
   Example: A student council member refrains from sharing classmates' personal information on social media and educates others on the importance of privacy settings to protect personal data.
3. Ethical Standards and Integrity: Good leaders act ethically and with integrity. Online, this means respecting others' privacy and not engaging in harmful activities like cyberbullying.
   Example: A student council member promotes a "No Cyberbullying" pledge and makes sure to report any harmful behavior they see online.
4. Communication and Education: Effective leaders communicate well and educate others. They can teach their peers about staying safe online and the importance of cybersecurity.
   Example: A class president organizes a workshop on cyber safety, teaching students how to recognize phishing attempts and the importance of not oversharing personal information online.
5. Crisis Management and Incident Response: Leaders are trained to handle crises calmly. This is useful if something goes wrong online, like getting hacked.
   Example: A scout troop leader knows what to do if their social media account gets hacked: They immediately change their password and inform an adult.

6. Promoting a Cyber-safe Culture: Leaders help create a culture of safety and respect. They encourage their peers to follow good online habits.
   Example: A school play director includes a rule in the rehearsal agreement that cast members should keep their social media profiles private to protect their personal information.
7. Role Modeling: Leaders lead by example. By practicing good cyber hygiene, they set a standard for others.
   Example: A science club president always logs out of shared computers at the library, encouraging others to do the same.
8. Collaborative Efforts and Teamwork: Leadership involves working well with others. This means encouraging friends to report suspicious activities and helping each other stay safe online.
   Example: A group project leader creates a group chat where everyone agrees to only share school-related information and to report any strange messages.

Advancing Online Cyber-Secure Behavior

These skills contribute to advancing online cyber safety in several distinctive ways…

1. Avoiding Oversharing: Just like a good leader doesn't share team secrets, a student learns not to overshare personal details like their home address or phone number online.
2. Recognizing Fake Friends: A leader learns to trust the right people. Similarly, students learn to recognize fake accounts or strangers trying to befriend them online.
3. Standing Up Against Cyberbullying: Leaders stand up for others. If a student sees someone being cyberbullied, they report it to a trusted adult[II] and support the victim.
4. Using Strong Passwords (or better yet, passphrases): Leaders know the importance of security. Students can learn to use strong, unique passwords and eventually use passphrases and change them regularly to protect their accounts.
5. Keeping Personal Information Private: Just like leaders keep important information confidential, students learn not to share personal information publicly on social media.
6. Encouraging Friends to Be Safe: Leaders inspire others. Students can encourage their friends to follow good online, cyber-safe practices, like not clicking on suspicious links or sharing passwords.

Leadership and Good Character

As students grow into leadership roles, they naturally start to become more independent in both their social and academic lives. By taking on responsibilities, they show they're ready to help others, listen with empathy, and make solid decisions. This development is crucial because it builds and sustains good character.

When students step up as leaders, they learn that leadership isn't just about being in charge. It's about leading by example, whether that's on a sports team or simply doing the right thing even when no one is watching. They come to understand that true leadership involves a lot of responsibility and is closely tied to having a strong character.

Learning leadership skills does more than just help students grow personally; it also enhances how they interact with others. They start to see the importance of looking out for their classmates, resolving social issues with the teacher's guidance, and making positive choices like joining team sports or participating in class discussions. These experiences help them build good character traits such as integrity, empathy, and reliability.

[II] This and subsequent chapters refer to "trusted adult" and that language is intended to be inclusive of legal guardians and caregivers of minors to also include … mentors, counselors, advisors, coaches, family friends, stepparents, foster parents, and teachers.

By developing these leadership and character traits, students not only improve their own lives but also contribute to a more supportive and cohesive school environment. This combination of leadership and good character prepares them to handle future challenges and succeed in various aspects of life.

Ethics: A General Introduction and Overview

Before we provide a generally accepted definition of ethics, we must examine the core principles that, when working together, lead to this generally accepted definition of ethics.

Defining Values

Core Principle #1 — Values. Values are the foundation of a person's ability to judge between right and wrong, they frame the decisions we make. Values include a deep-rooted system of beliefs that guide a person's decisions. They form a personal, individual foundation that influences a particular person's behavior.[10]

Values are "judgments of worth," moral principles, that should have a certain weight in the choice of an action. Values are individual beliefs that motivate people to act one way or another. They serve as a guide for human behavior.

Generally, people are predisposed to adopt the values that they are raised with. People also tend to believe that those values are "right" because they are the values of their particular culture.

Ethical decision-making often involves weighing values against each other and choosing which values to elevate. Values are universally recognized as a driving force in ethical decision-making.[11]

Defining Morals

Core Principle #2 — Morals. Morals are the principles that guide individual conduct within society, and they emerge from core values. While morals may change over time, they remain the standards of behavior that we use to judge right and wrong.

In the study of ethics, the terms amoral and immoral are often interchanged; however, in application, they are quite different.

Amoral refers to a lack of moral principles or a disregard for moral values altogether. When someone or something is described as amoral, it means they do not differentiate between right and wrong, nor do they consider ethical implications in their actions.

Immoral, on the other hand, refers to behavior that is in direct violation of accepted moral principles or standards. Immoral actions are considered wrong or unethical and often lead to negative consequences for others or society as a whole.

Amoral behavior lacks a moral compass altogether, whereas immoral behavior knowingly goes against established moral standards. While amoral actions may not carry inherent moral judgment, immoral actions are generally seen as wrong and ethically objectionable.

In general, morals are concerned with what people believe to be right and good conduct and are transmitted from generation to generation, evolving and being reinterpreted for each age. This broad understanding of what is right and wrong in human conduct is taught to us by our families, religion, national culture, and legal structure.

Morals refer to what is judged as right, just, or good. Judgment is the ability to make accurate determinations. Norms state what is morally correct behavior in a certain situation. Standards assess and measure ethical behavior. Working together, these five core principles lead us to a generally accepted definition of ethics.[12]

Defining Judgment

Core Principle #3 — Judgment. Judgment refers to the process of evaluating and making decisions about the moral rightness or wrongness of an action, behavior, or belief. Ethical judgment involves considering various moral principles, values, and standards to assess whether a particular action is morally permissible, obligatory, or prohibited. Ethical judgment consists not of getting the right answers all the time, but … of consistently asking the right questions.

The American Psychological Association (APA) defines ethical judgment as a moral decision made by an individual, especially a difficult one made in the context of a real or hypothetical ethical dilemma. Such judgments often reveal an individual's beliefs in discriminating between right and wrong and the attitudes that comprise their basic moral orientation.[13]

Defining Norms

Core Principle #4 — Norms. Norms refer to the established standards, rules, or principles that govern and guide human behavior within a particular social or cultural context. These norms dictate what is considered morally acceptable or unacceptable within a given community, group, or society. Norms serve as a framework for evaluating and judging the ethicality of actions, decisions, and practices. These norms help to promote ethical conduct and help prevent harmful or unethical behaviors.[14]

Cultures can encompass both ethical and unethical customs, expectations, and behaviors. It is important to recognize that cultural norms vary significantly across different societies, and what may be considered acceptable in one culture may not be in another. When teaching middle school students about ethics, educators should emphasize that while assessing norms, it is crucial to understand how one's ethical views can be influenced and sometimes limited by one's own cultural perspective or background. This understanding should go hand in hand with being culturally sensitive to others, recognizing that cultural diversity often brings different, and sometimes conflicting, viewpoints on what may be right or wrong.

However, ethics should not be confused with merely following culturally accepted norms. Some cultures uphold ethical standards that promote fairness, kindness, and justice, while others may have customs or practices that are unethical or harmful.

For example, students can learn about historical instances where cultural norms were unethical, such as the practice of slavery in the United States before the Civil War. These discussions can help students understand that just because something is widely practiced or accepted within a culture does not make it ethically right.

Educators can introduce the concept that ethical standards should be based on universal principles of right and wrong, rather than simply adhering to the norms of the time or place. The phrase "When in Rome, do as the Romans do" is not an adequate ethical standard because it suggests that one should conform to the behavior of others without critically assessing whether that behavior is morally acceptable. Instead, students should be encouraged to think critically about cultural norms and to develop their own ethical framework based on principles such as justice, equality, and respect for all individuals.

In presenting the topic of morals and relating it to concepts identifiable to middle school students, educators should consider using examples that resonate with their students' experiences. For instance, educators can discuss peer pressure and how, sometimes, just because everyone in a peer group is doing something, doesn't mean it's the right thing to do. Educators can also discuss how students from different cultural backgrounds might have different views on issues like fairness or respect, and how understanding and respecting these differences is part of being an ethical leader.

By teaching students to critically evaluate cultural norms and to stand up for what is right, educators can help students develop the skills they need to be ethical leaders in their communities, both online and offline. This not only fosters moral development but also encourages students to become more thoughtful and compassionate individuals capable of navigating the complexities of our increasingly diverse and digitally connected world.

Defining Ethical Standards

Core Principle #5 — Standards. Standards refer to the specific criteria or benchmarks that are used to assess and measure ethical behavior or the moral quality of actions, decisions, or practices. These standards serve as guidelines for evaluating whether an individual, organization, or society is adhering to ethical principles and behaving in a morally responsible manner. Standards are crucial in promoting ethical behavior and holding individuals and institutions accountable for their actions, ensuring that they align with recognized ethical values and principles.

Ethical standards are a set of principles and guidelines that help individuals and organizations determine what is right, wrong, fair, and just in their behavior and decision-making. These standards are based on values such as honesty, integrity, fairness, respect, responsibility, and accountability. Ethical standards can be formalized in codes of conduct, organizational policies, professional guidelines, or laws, but they can also be informal norms that govern behavior within a community or group.

In our digitally connected and dependent world, where the boundaries of right and wrong can often blur, ethical standards offer a consistent framework for making righteous decisions. They provide clarity in traversing complex cyber scenarios, such as data privacy, cybersecurity, and digital communication. In a digital society, observing ethical standards is crucial for fostering trust among users, organizations, and the broader online community. When people are confident that others will act ethically, it strengthens social bonds and facilitates smoother interactions in digital spaces, whether in personal, professional, or public contexts.

Ethical standards play a vital role in ensuring that actions and decisions in cyberspace are fair and just. They help protect individuals from online harm, exploitation, and discrimination, contributing to a more equitable digital society. Although ethics and law are not identical, many ethical principles form the basis of society-driven legal regulations that govern cyberspace. Adhering to ethical standards helps organizations and individuals comply with these laws, reducing the likelihood of legal repercussions and enhancing overall cyber safety.

Ethical standards operating in a digitally connected and dependent world encourage individuals and organizations to consider the broader impact of their actions on society and the environment. This sense of responsibility is crucial for addressing challenges such as digital inequality, cyberbullying, and environmental sustainability in technology use. These topics will be addressed more completely in the following chapters.

By establishing clear boundaries of acceptable digital behavior, ethical standards are instrumental in mitigating harm in online environments. They promote actions that protect the well-being and dignity of all digital stakeholders, from individuals to entire communities.

Ethical standards are indispensable to an efficient operational functioning, and cyber safety digital environment. Ethical standards provide the moral guidance needed to navigate the complexities of the digital world, foster trust, promote fairness, mitigate and protect against harm, and contribute to a just and responsible online society.

In summary, ethics is the collection of values, morals, judgments, norms, and standards, which provides a framework for acting (see Figure 1.2).

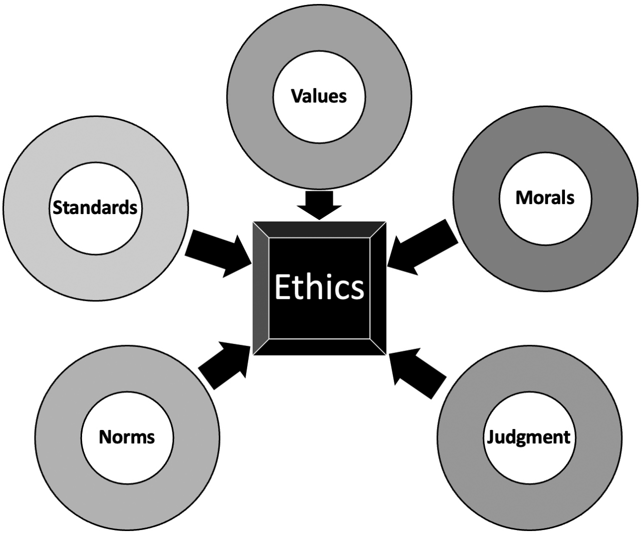


Figure 1.2 Core principles of ethics.[15]

Ethics, Trust, and Cyber Safety

We just discussed ethics and the essential core principles that ethics embodies. One remaining element to discuss is that of "trust."

The mutualistic relationship between ethics, trust, and cyber safety is crucial in creating a secure and reliable digital environment. Each element supports and enhances the others, leading to a more robust and trustworthy digital society.

Ethics in the context of cyber safety involves adhering to moral principles and guidelines that promote honesty, integrity, and respect in digital interactions. Ethical behavior ensures that individuals and organizations act responsibly, protect sensitive information, and respect privacy.

Trust is built when individuals and organizations consistently demonstrate ethical behavior online. Trust is essential for effective communication, collaboration, and transactions in the digital world. When users trust that their data are secure and that others will act ethically, they are more likely to engage positively with digital platforms.

Cyber safety encompasses the measures and practices put in place to protect users from online threats such as hacking, phishing, and identity theft. Effective cyber safety strategies rely on both trust and ethics. When users follow ethical guidelines and trust that these guidelines are being enforced, the overall security of the cyber environment is enhanced.

Mutualistic Relationship between Ethics, Trust, and Cyber Safety — Examples

1. Ethics Promotes Trust:
    - When individuals and organizations act ethically, they build a reputation for reliability and honesty. This behavior fosters trust among users, as they feel confident that their interactions and data are handled responsibly.
    - Example: A company that transparently communicates how it uses customer data and implements strong data protection measures builds trust with its customers.
2. Trust Enhances Cyber Safety:
    - Trusting relationships encourage users to follow cyber safety guidelines and report suspicious activities. When users trust that their actions contribute to a safer digital environment, they are more likely to engage in behaviors that protect themselves and others.
    - Example: Employees who trust their organization's cybersecurity policies are more likely to follow protocols, such as not sharing passwords and reporting phishing attempts.
3. Cyber Safety Reinforces Ethics:
    - Strong cyber safety measures support ethical behavior by providing a secure framework within which users can operate. When users know that ethical guidelines are enforced through robust cybersecurity practices, they are more likely to adhere to those guidelines.

- Example: Schools that implement strict cybersecurity measures and educate students about ethical online behavior create a culture of respect and responsibility.

Ethics, trust, and cyber safety are interconnected in a mutually beneficial relationship. Ethical behavior builds trust, which in turn encourages adherence to cyber safety practices. Effective cyber safety measures reinforce the importance of ethical behavior, creating a secure and trustworthy digital environment. By understanding and promoting this relationship, educators, organizations, and individuals can contribute to a safer and more reliable online world.

Ethics and Leadership

Ethics and leadership share a mutualistic relationship when it comes to being cyber-safe.

Ethics refers to understanding the difference between right and wrong and making choices that reflect this understanding.

Educators may present this mutualistic relationship to their students in such a manner…

> Ethics in cyber safety means doing the right thing online, even when no one is watching. It includes respecting others' privacy, not spreading false information, and not engaging in harmful behaviors like cyberbullying.
>
> Leadership is about guiding others and setting a good example. When combined, these qualities help create a safe and respectful online environment. Leadership involves setting a good example for others to follow. When leaders act ethically online, they show others how to be responsible digital citizens.

Mutualistic Relationship between Ethics and Leadership — Examples

Example 1: Respecting Privacy

- Scenario: Imagine you find out your friend's email password. An ethical decision would be not to log into their account. A good leader would also remind others not to invade someone's privacy.
- Discussion Point: Talk about why respecting others' privacy online is important and how invading it can cause harm. Discuss how you can set a good example by not sharing passwords or personal information without permission.

Example 2: Avoiding Cyberbullying

- Scenario: You see a classmate being bullied online. An ethical leader would not join in and would instead support the victim by reporting the bullying to a trusted adult.

- Discussion Point: Discuss why cyberbullying is wrong and how it affects people. Encourage students to think about how they can lead by example by standing up against cyberbullying and supporting their peers.

Example 3: Sharing Accurate Information

- Scenario: You come across a shocking news story on social media. Instead of sharing it immediately, an ethical leader checks if it's true by looking at reliable sources.
- Discussion Point: Explain the importance of not spreading false information. Talk about how sharing accurate information helps keep everyone safe and well-informed. Encourage students to always verify the facts before sharing news.

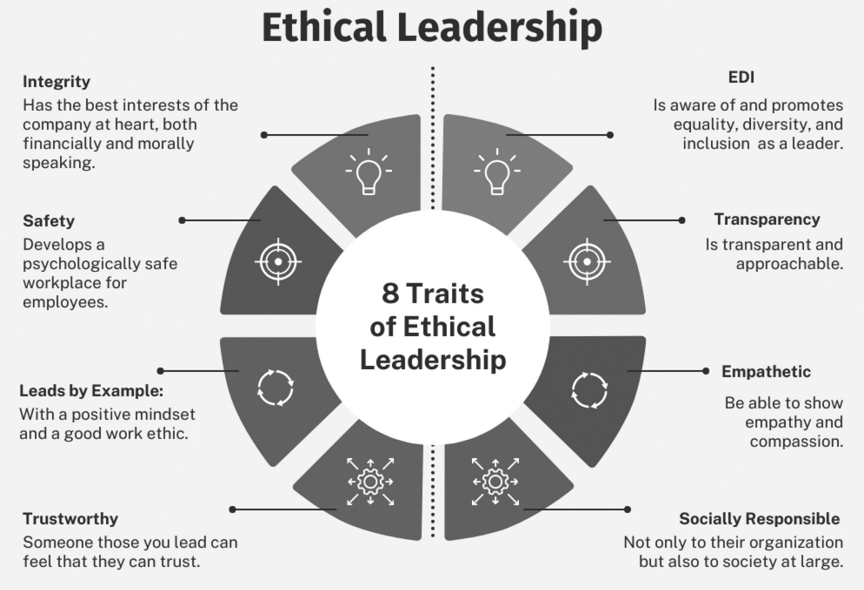
Ethical Leadership

> Ethical leadership is not defined by the task of making the right decision, but rather by whom one is.[16]

Researchers in the field of applied psychology define ethical leadership as the demonstration of appropriate conduct through personal actions and relationships and the promotion of such conduct to subordinates through two-way communication, reinforcement, and decision-making. This definition highlights three key components of ethical leadership.[17]

Dr. Valeria Lo Iacono, writing in "Ethical Leadership: A Cornerstone of Success in Business and Effective Managerial Training," states that ethical leadership is about being a leader. A leader who considers and works toward being that person who:

1. Has Integrity: Acts fairly and represents the company in a fair way (both for their financial interests and morally).
2. Works to **promote Equality, Diversity, and Inclusion (EDI)** within the workplace and is fair to all employees.
3. **Creates a safe work environment** for those one leads (i.e., a psychologically safe workplace).
4. Provides **transparency and is approachable**, i.e., enables open communication.
5. **Leads by Example**, including by showing honesty and through a good and positive work ethic and manner.
6. Can **show empathy and compassion** toward others.
7. Is someone whom others feel they **can trust**.
8. Is Socially Responsible: Ethical leaders recognize their responsibility not only to their organization but also to the greater society (see Figure 1.3).



Integrity
Has the best interests of the company at heart, both financially and morally speaking.

Safety
Develops a psychologically safe workplace for employees.

Leads by Example:
With a positive mindset and a good work ethic.

Trustworthy
Someone those you lead can feel that they can trust.

EDI
Is aware of and promotes equality, diversity, and inclusion as a leader.

Transparency
Is transparent and approachable.

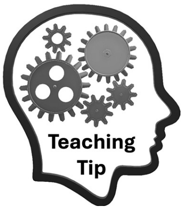
Empathetic
Be able to show empathy and compassion.

Socially Responsible
Not only to their organization but also to society at large.

Figure 1.3 Dr. Lo Iacono's eight traits of ethical leadership.[18]

Teaching Ethical Leadership to Middle School Students

Educators may wish to consider these steps and examples when preparing for class discussions on ethical leadership. This approach will assist students in understanding and embodying the principles of ethical leadership, preparing them to make responsible and positive contributions to their communities.



Teaching ethical leadership to middle school students involves helping them understand the importance of integrity, empathy, fairness, and social responsibility. By using relatable examples and interactive activities, educators can make these concepts accessible and relevant to these students.

Classroom Discussion on Ethical Leadership — An Approach

Step 1: Introduction to Ethical Leadership

- Objective: Define ethical leadership and explain why it is important.
- Activity: Begin with a class discussion asking students what they think makes a good leader.
- Example: Use a well-known figure (e.g., a teacher, coach, or community leader) as an example to highlight qualities like honesty, fairness, and empathy.

Step 2: Understanding Key Components

- Objective: Break down the key components of ethical leadership.
- Activity: Use real-life scenarios and stories to illustrate each component.
- Examples:
    - Integrity: Share a story about a student who found a lost wallet and turned it into the school office.
    - Empathy and Compassion: Discuss how a classmate helped a new student feel welcome.
    - Fairness: Talk about a teacher who ensures everyone has a chance to participate in class activities.
    - Social Responsibility: Highlight a student-led initiative, e.g., developing a school-wide program to clean up the local park.

Step 3: Role-Playing Exercises

- Objective: Allow students to practice ethical decision-making.
- Activity: Organize role-playing scenarios where students must make ethical decisions.
- Examples:
    - Scenario 1: A friend asks to copy homework. Discuss the importance of honesty and the potential consequences of cheating.
    - Scenario 2: A group project where one member isn't contributing. Discuss how to address the situation fairly and encourage teamwork.

Step 4: Group Projects and Discussions

- Objective: Foster collaboration and communication among students.
- Activity: Assign group projects that require ethical decision-making and teamwork.
- Examples:
    - Project 1: Plan a charity event for a local cause. Discuss the importance of social responsibility and community involvement.
    - Project 2: Create a classroom charter that includes rules for respectful and fair behavior. Encourage open communication and collective decision-making.

Step 5: Reflective Journaling

- Objective: Encourage self-reflection on personal values and actions.
- Activity: Have students keep a journal where they reflect on their daily actions and decisions.
- Examples:
    - Write about a time they had to make a difficult decision and how they handled it.
    - Reflect on a leader they admire and what makes that person ethical.

Step 6: Guest Speakers and Role Models

- Objective: Provide real-world examples of ethical leadership.
- Activity: Invite guest speakers who demonstrate ethical leadership in their professions.

- Examples:
  - A local business owner who practices fair trade.
  - A community leader who advocates for social justice and equality.

Step 7: Ongoing Conversations and Support

- Objective: Maintain an open dialogue about ethical behavior and leadership.
- Activity: Regularly check in with students about their experiences and challenges related to ethical leadership.
- Examples:
  - Weekly or biweekly class discussions on ethical dilemmas in current events.
  - Encourage students to share their reflections and discuss how they apply ethical leadership in their daily lives.

Ethical Principles for Seventh- and Eighth-Grade Students

In the quest for your students to achieve good character, leadership, ethical behavior, and proactively being cyber safety, seventh- and eighth-grade students should consider following these principles inspired by the traits of ethical leadership:

1. Integrity

   Principle: Always be honest and fair.

   Example: If you find something that doesn't belong to you, return it to a teacher or the lost and found.
2. EDI

   Principle: Treat everyone with respect and fairness, regardless of their background.

   Example: Include all classmates in group activities and stand up against bullying or exclusion.
3. Safety

   Principle: Create a safe and supportive environment for yourself and others.

   Example: Report any harmful or unsafe behavior you see online or in-person to a trusted adult.
4. Transparency

   Principle: Be open and approachable in your communications.

   Example: Share your thoughts and feelings honestly with friends and family and be willing to listen to theirs.
5. Leading by Example

   Principle: Set a positive example through your actions and behavior.

   Example: Show good sportsmanship in games, do your best in school, and be kind to others.
6. Empathy

   Principle: Show empathy and compassion toward others.

   Example: If a classmate is feeling down, offer your support and listen to them without judgment.

7. Trustworthiness
   Principle: Be someone others can trust.
   Example: Keep your promises and be reliable; if you say you will do something, make sure you follow through.
8. Social Responsibility
   Principle: Recognize your responsibility to contribute positively to your community.
   Example: Participate in community service projects, like helping to clean up a local park or organizing a charity event at school.
9. Cyber Safety
   Principle: Be mindful of your actions online to stay safe and protect others.
   Example: Use strong passwords, avoid sharing personal information, and never participate in cyberbullying.

By following these principles, students can develop the skills and attitudes necessary to become ethical leaders and responsible digital citizens. These principles not only help in personal growth but also in creating a positive and inclusive environment both online and offline.

Top Five Skills for Cyber Safety in the Mid-21st Century

Educators may wish to plan class discussions or exercises with students reinforcing these essential cyber safety skills.

Teaching Tip

1. Cybersecurity Literacy: Understanding the fundamentals of cybersecurity, including recognizing phishing attacks, creating strong passwords, and securing personal devices and networks.
2. Critical Thinking and Problem-Solving: The ability to analyze and respond to digital threats creatively and effectively, making informed decisions under pressure.
3. Digital Hygiene Practices: Regularly updating software, backing up data, and following secure protocols to minimize the risk of breaches.
4. Awareness of Social Engineering Tactics: Recognizing and resisting manipulation attempts through social engineering, which is increasingly sophisticated in the digital age.
5. Ethical Judgment and Decision-Making: Applying ethical principles to digital actions, ensuring that decisions respect privacy, data integrity, and the overall well-being of others in the digital space.

By learning, integrating, and adhering to these concepts and skills, students will be better able to navigate the challenges of a digitally connected, digitally dependent, and digitally evolving world while leading with integrity, acting ethically, and staying safe in the face of ongoing cyber threats.

As society completes the first quarter of the 21st century, as the world becomes increasingly interconnected and dependent on digital technologies, leadership, ethics, and taking a proactive stance on cyber safety are more crucial than ever.

Leadership in a Digital Age

- Vision and Innovation: A leader in this era must be forward-thinking, understand current technologies, and maintain an "educational involvement" with evolving technologies. This involves inspiring others to embrace change and innovate continuously.
- Empathy and Communication: Effective digital leadership requires clear communication and the ability to empathize with diverse groups of people across digital platforms. This fosters a culture of inclusivity and trust, even in virtual spaces.
- Decisiveness in Crisis: The rapid pace of digital transformation means that leaders must be able to make quick, informed decisions, particularly in the event of a cyberattack or data breach.

Ethics in a Digitally Connected World

- Data Integrity and Privacy: An ethical individual respects and upholds the privacy of others, understanding the critical importance of data integrity in maintaining trust within digital ecosystems.
- Transparency and Accountability: Ethical behavior in the digital age involves transparency in actions, decisions, and the use of technology. It also means taking accountability for mistakes, particularly those that impact others' digital lives.
- Responsibility and Stewardship: Ethics demands that individuals act responsibly with the power that digital tools provide, avoiding harm and working toward the common good in all digital interactions.

Maintaining a Proactive Position on Cyber Safety

- Continuous Learning and Adaptation: A proactive individual remains up-to-date with the latest cybersecurity trends, threats, and best practices. This requires a commitment to continuous education and adaptation.
- Risk Management and Mitigation: Proactively managing risks involves identifying potential vulnerabilities and taking steps to mitigate them before they can be exploited.
- Resilience and Recovery: Proactivity in cyber safety includes not only preventing incidents but also developing and implementing effective recovery plans to quickly restore normalcy after an attack.

Who Is Generation Alpha?

As our Grades 7 and 8 children move from tweens to their teens, we have a new dilemma — how to curb their "honey-badger" independent approach? This generation, Generation (Gen) Alpha, is also known as the "honey badger" generation, born after 2010 (and through 2025). As parents.com writer Beth Ann Mayer explains, the term became popular on TikTok, and parents weighed in on it. One parent, Laura Loray, LCSW, PMHNP-BC, a New Jersey-based psychiatric nurse practitioner, is credited with making the term popular. This generation is described as strong-willed, ambitious, spicy, and confident. Loray continues,

> They are persistent seekers of justice, and as a result, will stand up to someone three times their size without hesitation. They are fearless, tenacious, always go after what they want without a second thought, and never back down from a challenge.[19]

Although these are impressive attributes to have in certain circumstances, they can have a negative impact when trying to enforce online restrictions and emphasize the cautions needed in today's online world. Since birth, this generation has consumed information via social media and online sources. They know influencers from the earliest ages and product marketing campaigns are built around them. How do teachers, guardians, parents, and even authors connect this group to the realities of cyber risks, and unacceptable and bullying behavior online?

Gen Alpha advocates for others, themselves and their environment according to a survey of 1025 kids by GWI.com. "What other people think of me" — social perception — received the lowest response rate (32%) of all questions asked with helping people (61%) and keeping people from being bullied (51%) receiving the highest response rate.[20]

These encouraging rates suggest that Gen Alpha is receiving the message!

Behavior — What Is Acceptable/Unacceptable?

Anti-Bullying

What Is Bullying? The Anti-Bullying Alliance and its members have an agreed shared definition of bullying based on research from across the world over the last 30 years.

> The repetitive, intentional hurting of one person or group by another person or group, where the relationship involves an imbalance of power. Bullying can be physical, verbal, or psychological. It can happen face-to-face or online.[21]

School bullying takes on many forms and may take place in various locations, however, the initial relationship between parties was formed in a school setting. Bullying may also be in the form of direct, in-person contact where it is more verbal, or indirect contact such as cyberbullying. It is important to ensure students understand that teachers, counselors, and all support systems within the school, or agency, are available for help and counseling regardless of where the bullying activity takes place, making school a safe environment.

Bullying impacts not only the ability to focus and learn but also physical and mental health, both while the bullying activity is taking place and in the long term.

The monitoring of bullying activities must be an ongoing activity in the classroom, on school grounds, and during school-sanctioned activities, and is supported school-wide. Successful monitoring requires a unified classroom plan that is aligned with and supported by the school's administrative plan.

According to the US Government Accountability Office (GAO), each year, millions of K—12 students experience hostile behaviors like bullying, hate speech, hate crimes, or assault. In school year 2018–2019, about 1.3 million students, ages 12–18, were bullied for their race, religion, national origin, disability, gender, or sexual orientation.

GAO's analysis of nationally generalizable surveys of students and schools. About one in five students aged 12–18 were bullied annually in school years 2014–2015, 2016–2017, and 2018–2019. Of students who were bullied in school year 2018–2019, about one in four students experienced bullying related to their race, national origin, religion, disability, gender, or sexual orientation. About one in four of all students aged 12–18 saw hate words or symbols written in their schools, such as homophobic slurs and references to lynching.

Most hostile behaviors also increased in the school year 2017–2018, according to the GAO analysis of the school survey. Hate crimes — which most commonly targeted students because of their race and national origin — and physical attacks with a weapon nearly doubled (see Figure 1.4 Hostile Behaviors in K—12 Public Schools, School Years 2015–2016 to 2017–2018). Sexual assaults also increased during the same period.

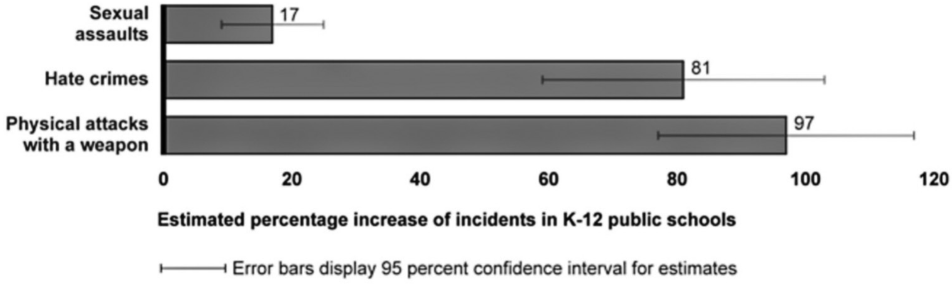


Figure 1.4 GAO report — hostile behaviors in K—12 public schools.[22]

So prevalent, all 50 U.S. and many US Commonwealths and Territories have anti-bullying laws and/or policies.[23]

Incidents of harassment or hate may include bullying by race, color, national origin, sex (including sexual orientation and gender identity), or disability status amongst others (see Figure 1.5).

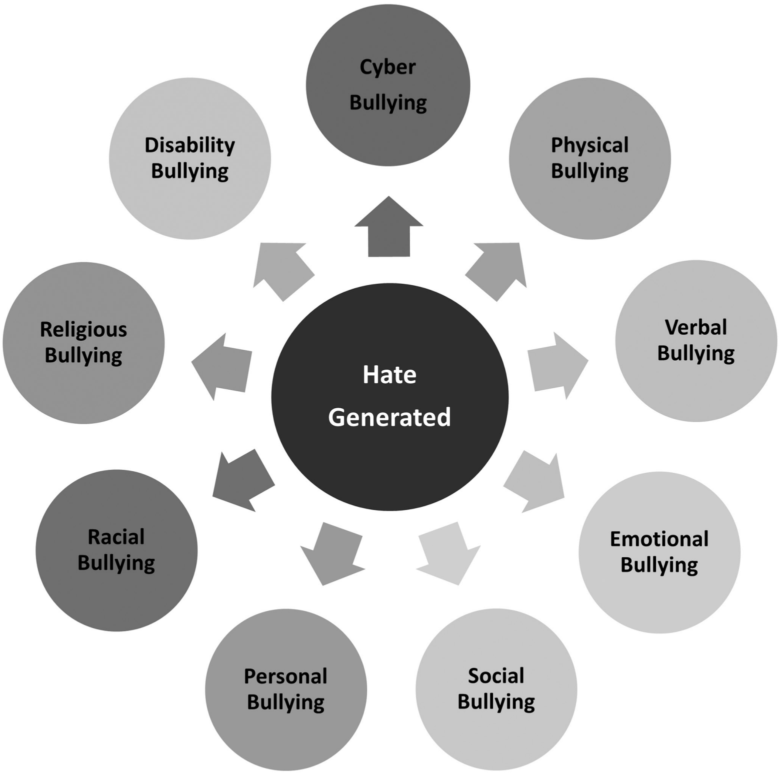

Cyber Bullying
Physical Bullying
Verbal Bullying
Emotional Bullying
Social Bullying
Personal Bullying
Racial Bullying
Religious Bullying
Disability Bullying
Hate Generated

Figure 1.5 Hate generated bullying.[24]

Margo Crawford, LCSW, discusses the emotional response to disturbing, terrifying, or life-threatening events. The stressful event can lead to trauma, which may dissipate over time. There are several types of trauma, which Crawford describes as follows:

> Acute trauma happens when the event is sudden and severe and leads to immediate emotional distress. After 6 months of experiencing symptoms, it is then classified as post-traumatic stress syndrome. Not all trauma leads to post-traumatic stress disorder (PTSD).
>
> Chronic trauma occurs when there is an extended period where persistent stressors exist such as hostile environments.
>
> Complex PTSD or CPTSD is categorized by more than one traumatic event within one's lifetime or a prolonged series of events.
>
> Secondary trauma is caused when a person has indirect exposure to a traumatic event, such as hearing someone's stories, being involved in some level of intervention, or witnessing a person's strong emotions related to a traumatic event.

When not addressed and the trauma continues, the stress level increases. Teachers, administrators, and parents may have secondary trauma via the indirect exposure to hearing or viewing their student's bullying activity.[25]

Newport Academy provides these ten signs of bullying to help identify if a teenager is being bullied. Teachers can watch for changes in student's behavior. Teens may have one or more symptoms of bullying or may have marked changes in other behaviors. While the signs of bullying listed below are not a guarantee that a teen is being bullied, knowing what to look for can help find out what is happening.

Signs that a teen is being bullied include

1. unexplained cuts, scratches, or bruises;
2. missing, damaged, or torn belongings;
3. loss of appetite or changes in appetite;
4. frequent stomachaches, headaches, or other physical complaints;
5. trying to get out of going to school or after-school activities;
6. reduced interest in school, or poor grades;
7. seeming sad, moody, or depressed, especially after school;
8. exhibiting anxious behaviors;
9. decreased self-esteem;
10. withdrawing from friends and social activities.

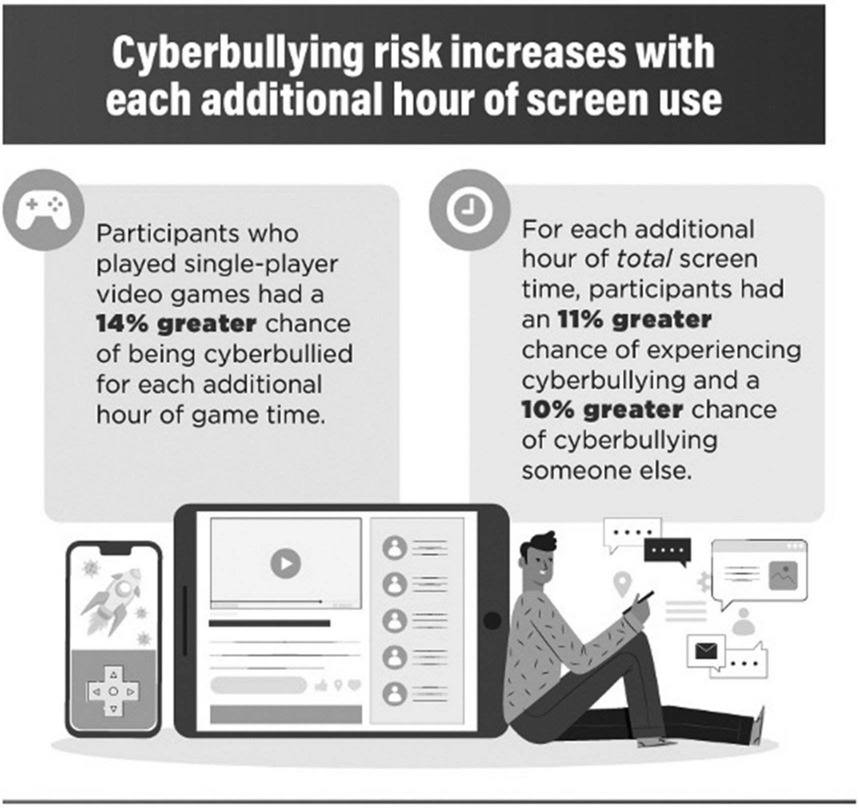
If you notice any of these signs, it's critical to have a conversation with the student about whether they are experiencing physical bullying, verbal bullying, or other types of bullying behavior, such as mean girl behavior or gaslighting.[26]

Notify your school administration and refer to your school or school district policy. If there is an imminent threat of any kind, report the activity to authorities immediately.

The following discussion and the lesson plans included in this chapter incorporate the following anti-bullying types and definitions. This is not an all-inclusive list of anti-bullying types and is a compilation of bullying types from the University of the People[27] and the Preventing and Promoting Relationships & Eliminating Violence Network (PREVNet).[28]

Although many of the types of bullying listed may appear to be direct, in-person bullying, they may also take place indirectly online via social media sites, email and text messages, and chatroom links often found through video games. Online bullying reflects direct, in-person bullying, and often moves online where the bully feels protected behind the screen allowing them to be even more aggressive. The types of bullying highlighted below provide a glimpse of direct, in-person behaviors and also how they may transfer to online bullying.

The National Institutes of Health (NIH) and the Adolescent Brain Cognitive Development^{SM} Study indicates that the cyberbullying risk increases with each additional hour of screen time as shown in Figure 1.6.



Cyberbullying risk increases with each additional hour of screen use

Participants who played single-player video games had a **14% greater** chance of being cyberbullied for each additional hour of game time.

For each additional hour of *total* screen time, participants had an **11% greater** chance of experiencing cyberbullying and a **10% greater** chance of cyberbullying someone else.

Figure 1.6 Cyberbullying risks.[29]

Cyberbullying: Cyberbullying is any type of bullying that happens online. It can be hurtful comments on a personal site or deceptive private messaging. It includes the use of email, cell phones, text messages, and Internet sites to threaten, harass, embarrass, socially exclude, or damage reputations and friendships.

Disability Bullying: This includes leaving someone out or treating them badly because of a disability, making someone feel uncomfortable, or making jokes to hurt someone because of a disability. On a physical level, it includes harmful actions such as blocking ramps and elevators, tripping, or tampering with accessible equipment. Online disability bullying may include making jokes to make the individual feel uncomfortable or "less than" and circulating memes of disabled people in a way that makes fun of the individual's disability.

Emotional Bullying: Emotional bullying involves using ways to cause emotional hurt to another person. This can include saying or writing hurtful things, causing others to gang up on an individual, and purposely ignoring, or spreading rumors. Online emotional bullying may include addressing comments directly to the person via social media sites or chat rooms with the intent to embarrass the person.

Personal Bullying: Personal bullying refers to any sort of bullying, done in any manner that is related to a person's gender or sexuality, including leaving someone out; treating them badly or making them feel uncomfortable because of their sex; making sexist comments or jokes; touching, pinching, or grabbing someone in a sexual way; making crude comments about someone's sexual behavior or orientation; or spreading a sexual rumor. Online personal bullying may include direct comments regarding the victim's appearance, hair, clothing, or general style. It may include manipulating the victim's accounts and posting comments as if they are the account owner. This may include hacking the person's account to appear as the account owner.

Physical Bullying: This always involves physical contact with the other person. This can mean hand-to-hand, but it can also mean throwing items, tripping, or eliciting others to cause physical harm to a person. This type of bullying can also cause harm to property and belongings.

Racial Bullying: This includes treating people badly because of their racial or ethnic background, saying bad things about a cultural background, calling someone racist names, or telling racist jokes. Online racial bullying may include "flaming" where language and insults are used to insult or intimidate the target.

Religious Bullying: This includes treating people badly because of their religious background or beliefs, making negative comments about a religious background or belief, calling someone names, or telling jokes based on his or her religious beliefs to hurt them. Online religious bullying may include making jokes about their belief to make them feel uncomfortable and posting demeaning memes of religious dress, food, or leaders.

Social Bullying: This includes rolling your eyes or turning away from someone, excluding others from the group, getting others to ignore or exclude, gossiping or spreading rumors, setting others up to look foolish, and damaging reputations and friendships. Online social bullying may include creating fake events like a party and posting pictures of friends to make the victim feel excluded from the event, or fake accounts in someone the victim's name to post negative or inappropriate comments or images.

An Example of social bullying, on a public stage may include how after a 2024 television event, a young neurodivergent son "broke the internet" when displaying his tearful love for his dad. Then the bullying began, primarily on social media platforms.

Nancy Doyle, a UK psychologist specializing in the neurodivergent conditions, says neurodivergent people tend to be highly sensitive and experience life at the extreme ends … that was "joyful to watch" as well casting a welcome spotlight on different people's experiences. "It gives us an opportunity to discuss the issue," says Doyle, who characterizes neurodiversity as an area that is as politicized as gender and diversity. "Expressing emotion is seen as weak because there are so many messages in society to repress, ignore or overcome emotional thinking."[30]

This young man's sudden fame focused attention on challenges of people with learning disabilities and how we choose to respond.

Verbal Bullying: Verbal bullying means using any form of language to cause the other person distress. Examples include using profanities, hurtful language, negatively commenting on a person's appearance, using derogatory terms, or teasing. Online verbal bullying may implement this type of language and include a call to action for others to join the verbal abuse against the person being bullied.

The Centers for Disease Control and Prevention indicates that different types of violence are connected and often share root causes. Bullying is linked to other forms of violence through shared risk behaviors. Addressing and preventing one form of violence may have an impact on preventing other forms of violence.[31]

The GAO was asked to review hostile behaviors in K—12 grades. Hostile behaviors, including bullying, harassment, hate speech, and hate crimes, or other types of victimization like sexual assault and rape, in schools can negatively affect K—12 students' short- and long-term mental health, education, income, and overall well-being.

According to guidance, incidents of harassment or hate, when motivated by race, color, national origin, sex (including sexual orientation and gender identity), or disability status can impede access to an equal education. In certain circumstances, these kinds of incidents may violate certain federal civil rights laws, which Education's OCR is tasked with enforcing in K—12 schools.[32]

School bullying is a global concern. As such, UNESCO Member States declared the first Thursday of November, the International Day against Violence and Bullying at School, including Cyberbullying, recognizing that school-related violence in all its forms is an infringement of children and adolescents' rights to education and their health and well-being.[33]

Activity

This presents a great opportunity for schools and child-serving organizations to create an activity or learning fair around this day for student, family, and community awareness. UNESCO themes each year and an activity or event may be created around the global theme. By incorporating the theme, students may create poster boards and drawings depicting bullying to display on the school premises such as halls, or in school/community events.

Encourage students to be creative. There are several free sites available students make use to make posters. Canva.com, sway.com and Adobe are several popular sites, and a quick Internet search will provide others.

Students can make a large visual exhibit with individual groups of students each designing and making a section of a larger exhibit based on the UNESCO theme. When displayed, the individual designs create a cohesive presentation.

Another exercise that may help students talk about bullying, is creative writing. Some students may find writing a healthy outlet to convey and process how they feel.

Everyone has a preferred way to communicate, and by offering a variety of options, each student will be able to express their feelings, concerns and needs for moving forward.

Your Role in Monitoring and Stopping Bullying

If there is an imminent threat of any kind, report the activity to authorities immediately.

Working with your school superintendent and governmental agencies is a starting point for developing a strategy for addressing bullying behavior. Currently, no federal law directly addresses bullying. In some cases, bullying overlaps with discriminatory harassment, which is covered under federal civil rights laws enforced by the US Department of Education and the US Department of Justice. No matter what label is used (e.g., bullying, hazing, teasing), schools are obligated by these laws to address conduct when it meets all three criteria below.

- It is unwelcome and objectively offensive, such as derogatory language, intimidation, threats, physical contact, or physical violence.
- It creates a hostile environment at school. That is, it is sufficiently serious that it interferes with or limits a student's ability to participate in or benefit from the services, activities, or opportunities offered by a school.
- It is based on a student's race, color, national origin, sex, disability, or religion.[34]

Every state and most US territories have some level of Anti-Bullying Laws, Policies, and Regulations. The common components found in state laws, policies, and regulations, which have evolved, include definitions of bullying, defining characteristics that are commonly targeted for bullying behaviors, and detailed requirements for school district policies. A table of state and territory common components is available at Common Components in State Anti-Bullying Laws, Policies and Regulations, StopBullying.gov.[35]

Teaching Tip

These steps are offered for consideration in developing a school plan for addressing bullying in your school. Add what is appropriate in your school and your community, it is an organic process, subject to revision, and enhance as needed.

1. Ensure you have your school administration's support.
2. Contact your school district to determine what policies, guidance, and support are currently available.
3. Who will be responsible for directing the policy development?
4. Who will be involved in the development process? Teachers and administration only? Include students? Parents and guardians? Law enforcement? Professional service agencies that deal with adolescents and bullying?
5. Establish the objective(s) of your anti-bullying policy.
6. Determine the goals you wish to achieve. Consider the SMART goals method — Specific, Measurable, Achievable, Relevant, and Timely.
7. Understand and plan your policy's vetting process for fairness and to ensure the policy complies with federal and state laws.
8. What type of mediation will be available to students — both those being bullied and the bully?
9. When will intervention be required? Are there specific triggers for automatically calling law enforcement or a professional agency?

10. What is the process to determine what organizations to contact for referral?
11. Decide how you will implement your anti-bullying policy.
12. What metrics will be used to establish that the policy is working?
13. How frequently will the policy be reviewed for currency and compliance with changing federal and state laws?
14. Who is responsible for managing and maintaining the anti-bullying policy?

These steps will begin the process of ensuring your school is proactive in safeguarding all students from bullying behavior.

"But I Was Just Teasing." Teasing and Bullying

As is often the case, when confronted, many bullying responses include "I was just teasing," or the victim may also try to diminish the incident with the response "Don't make a big deal of it, they were just teasing." The line between teasing and bullying may be easily crossed, if not managed properly.

Sometimes teasing is harmless and playful. Other times it can be used to hurt others. Even playful teasing can hit raw nerves or be misinterpreted, especially when kids struggle with social skills. Many kids tease each other to bond or form relationships. The teasing shows each other they can joke around and still be friends.

But teasing can also be used to communicate the negative. It's often used to establish "top dog" amongst kids — an imbalance of power. Also, what's playful to one child may not feel playful to another. In those cases, teasing can lead to hurt feelings. Another distinct difference between teasing and bullying is that bullying is repeated; it continues with regularity, even after the subject of the bully has indicated it is not appreciated or taken playfully.

With these negatives, why not discourage teasing completely? Like any communication, teasing has its purpose. Some topics that are awkward to raise in serious conversation are easier to raise through teasing.

- Teasing and bullying are different.
- Not all teasing is bad. Sometimes it's playful and helps kids bond.
- When teasing is meant to hurt and is done over and over, it can become bullying.

Verbal bullying is different from teasing. It's not done to make friends or to relate to someone. Just the opposite: The goal is to embarrass the victim and make the bully look better and stronger.

The tricky thing is that bullying may start as teasing. But when it's done over and over and is meant to be hurtful or threatening, it becomes bullying.

Unlike kids who are being bullied, kids who are being teased can influence whether it continues or ends. If they get upset and speak up, the teaser usually stops.

Sometimes, kids who are trying to tease end up bullying. For example, a child may say something mean-spirited to another, thinking it's playful. This can lead to an argument. Or a child may react angrily to a friendly comment, which may cause other kids to keep their distance. This failed attempt at teasing or humor may also escalate to an online social media attack started by either or both parties involved. Catching a failed teasing incident early is key to keeping it from escalating.

The San Bernardino Sun (CA) reports that there are school districts with much lower cyberbullying rates. Loretta Whitson, executive director of California Association of School Counselors, indicates that improved rates are typically a result of

- improving school mental health climates;
- hiring additional counselors;
- implementing more robust anti-bullying policies and procedures;
- taking what happens online as seriously as what happens on campus; and
- creation of online portals to report bullying and put links to them everywhere, including on students' district-issued devices, by posting QR codes around campus, and placing links on district and school websites.[36]

To address these struggles, it's important to teach kids about the rules of conversation. Help kids sort out when teasing is okay and when it becomes hurtful or borders on bullying. One way to do this is by role-playing with them. This lets kids practice a situation where they get teased, don't like it, and need to respond (Figure 1.7).

NEGGING
self-esteem
compliment
emotional manipulation
anxiety
emotions
negative
relationship
compare
abuse
insult
manipulation
comment
seduce
depression
ignore
behavior
confidence
feelings
backhanded compliment
undermine
neg
change
negging

Figure 1.7 Teasing words.[37]

Questions to Ask Kids about Teasing Maybe you've heard that kids are teasing a child or your student at school. You can ask a few questions to see whether it's good-natured or harmful:

- Are the kids who tease you your friends?
- Do you like it when they tease you?
- Do you tease them back?
- If you told them to stop teasing, would they?
- If you told them that they hurt your feelings, would they say they were sorry?

If the answer to any of these questions is "no" or "I don't know," then it may be a case of negative teasing or even bullying. It's important to find out more.[38]

Adults and peers can be an advocate for a person being teased or bullied. An advocate supports the cause or needs of others by considering that we are most effective when we are supporting each other.

How to respond to bullying situations is a good classroom activity to practice. This practice is a sound way to prepare students for a bullying situation. It may also make the bully aware of their behavior, and that is it neither appropriate nor appreciated. This is a guided practice and is not intended to make anyone feel bad or guilty.

The list indicating the different types of bullying, previously discussed, may be used to create bullying scenarios. Scenarios should not reflect any identifiable student.

Guided responses may include the following:

- "That is my friend and don't talk to them that way." Shows support and that there are allies.
- "I do not like you saying/doing that. Please stop." It is a firm statement and a request to stop. This is a good approach as the immediate response by the bully and future activity will also assist in determining if it is bullying or teasing.
- "I have asked you to stop before. I am reporting this to the teacher."
- "It makes me embarrassed when you say/do this."

It is not important who started any bullying actions or comments. What is important is how the recipient feels and the intention of the bully.

It is important not to be passive in our online interactions. We control what we consume, so a proactive approach is not to click on notices from people you don't know, open links you are not expecting including unexpected links from a trusted source, and not sharing anything personal with individuals or organizations asking for information (Figure 1.8).

kindness
respect
policies
community
youth
stop
training
physical
prevention
protect
safe
parents
efforts
children
signs
help
cyber
education
STOP BULLYING
environment
prevent
safety
groups
students
stand up
resources
organize
peers
behavior
watch
pledge
educate
educators
kids
friends
teens
schools
people
emotional

Figure 1.8 Stop bullying.[39]

In the following section, we take a closer look at what is good judgment and how we communicate this principle, this concept to young learners. Using good judgment is not only an important life skill but becomes especially important when navigating the oft-times confusing and perilous world of technology. Using good judgment is a primary cyber-safe skill!

Using Good Judgment by Making Good Decisions

Judgment and decision-making are an integral part of discussing character education. Character education is to guide students to make thoughtful choices and act with integrity. Creating an environment where students feel safe making choices and are guided in how to make good choices empowers the student to feel confident in making future choices.

Every choice or decision costs something — perhaps time, or money and resources, or one's reputation. All decisions, good and bad ones, come with a cost. Good judgment and good decision-making skills are the foundation to future ethical behavior when the stakes, i.e. the costs, are higher.

Peer Pressure

Influence

A study published by Cambridge University Press indicates that although peer influence is often conceptualized as harmful, teens influence one another to engage in various behaviors. Of course, these actions include antisocial behaviors such as lying, stealing, and cheating. At the same time, peers also influence each other to engage in prosocial behaviors such as helping, sharing, and cooperating. Finally, teens encourage peers to engage in risky behaviors such as substance use, which are not clearly categorized as prosocial or antisocial.

The study continues to suggest that we typically imagine peers influencing one another through the explicit encouragement of specific behaviors, a process termed direct influence. However, the mere presence of peers is enough to alter adolescent behavior, a phenomenon labeled indirect influence. In addition, even when teens are no longer in the presence of peers who directly influenced them, they may continue to engage in the behaviors that peers encouraged, a construct we call continuing influence.[40]

Susceptibility

Brett Laursen, Ph.D., fellow of the APA, untangles peer influence from peer susceptibility; there are some children who are susceptible to influence from anyone — that is to say that whatever comes down the pike they're likely to follow. But it's also the case that some people are more influential and so, if you hang around with people who tend to be particularly influential, you will look susceptible even though you're not particularly susceptible. It just happens to be that you're hanging around with others who are highly influential.

Hanging around with somebody who's very persuasive and who has a lot of social skills, you may look susceptible when in fact you're not particularly susceptible to other people. It just has to do with those that you spend your time with. So, we know that susceptibility is greater for children who don't have a lot of friends. They want to protect the friendships that they have, and so they're more likely to do what their friends say because they're worried about losing their friends and have difficulty making others.

Younger children who hang around with older children are susceptible to influence. Paradoxically, being popular may make you susceptible to influence. This one is a little bit up in the air, but it may be that popular kids in some domains worry about protecting their status and so, they're more likely to be influenced to be seen doing things that they should be seen doing even if they don't want to do them because otherwise they fear their status will diminish in the eyes of their peers.[41]

What Is Good Judgment?

Good judgment starts with knowing how to assess options and the consequences involved in making a choice. It is also important to convey that not all questions or actions must have an immediate answer. Taking time in responding and assessing the costs involved — tangible and nontangible — is part of developing good ethical decision-making skills.

Using good judgment as well as good decision-making is the foundation for ethical and moral decisions, the child will continue to make as they get older. The Menninger Clinic, a mental health facility in Houston, states that

> graduates get into the most elite colleges but can't handle college life emotionally—and so take a medical leave of absence and come to the Menninger Clinic for treatment and went on to say that all of these students had had insufficient experience making decisions for themselves, handling setbacks, and managing life's temptations independently.

Authors Johnson and Stixrud continue reinforcing the need for early decision-making skills, stating…

> So, while our impulse is to try to keep our kids safe, our priority as they get older should shift to helping them develop the skills—including the decision-making skills—they need to keep themselves safe, along with the confidence that they can trust their judgment and solve problems as they arise. In our view, the time to start supporting kids in making their own decisions isn't when we send them to college—it's when they're young—because we want them to have a ton of practice making and learning from their own decisions…[42]

As children are older, there is less control of the decision-making process by adults. But are adolescents ready to make decisions?

Neuroscience News shows scientific advances help us understand how adolescents carry out the decision-making process. Perhaps the most significant finding is that they do so with a brain that is still developing, so not all of its competencies are fully acquired. And this can lead to mistakes.

During adolescence, many situations require making decisions: trying something new, approaching another person we find attractive, or transgressing a rule established by the family. All these decisions involve two areas of the brain that mature at very different times. In their heads, a highly activated pleasure-seeking system is combined with a developing conscious behavioral regulation system and leads to decision-making that adults perceive as risky.

Scientific studies provide these three tips:

1. Making mistakes and taking certain risks is an adolescent process: The important thing is to learn from them.
2. The brain development of this age group means that the pleasure of experimenting with certain risky behaviors prevents a proper assessment of their consequences. It is necessary to explain, carefully and with understanding, what these consequences are.

3. Adolescents need to feel free to experiment and make mistakes, but they also need to know the limits and consequences. Although they want to be independent, they still need to feel cared for by the adults.[43]

Choices — Where to Start?

Children of all ages must make decisions. Understanding that adolescent brains are still developing helps appreciate that easy decisions for an adult could require skills a child may not have developed.

Based on the stage of their brain development, adolescents are more likely to

- act on impulse,
- misread or misinterpret social cues and emotions,
- get into accidents of all kinds,
- get involved in fights, and
- engage in dangerous or risky behavior.

Adolescents are less likely to

- think before they act,
- pause to consider the consequences of their actions, and
- change their dangerous or inappropriate behaviors.[44]

Do these sound familiar?

Does Gen Alpha Make Decisions Differently than Prior Generations?

Neuroscience News continues by summarizing the study, indicating that when making moral judgments of past actions, adults often think counterfactually about what could have been done differently.[45] Generally, children seldom reflect on this.

Understanding the characteristics of Gen Alpha will help discover their decision-making process. It is important to note that these characteristics can vary greatly among individuals within each generation and are not absolute.

- Tech-savviness: Gen Alpha is highly proficient with technology and the Internet; having grown up with even more advanced technology and the Internet, they are even more tech-savvy than Gen Z, especially over the past decade.
- Diverse: Gen Alpha is even more diverse and globally minded than Gen Z, which is already considered the most diverse generation in history. Gen Alpha is the first generation to be born into a world where technology and the Internet have always been a constant presence, making it easier to connect with people from different backgrounds and cultures. Additionally, many Gen Alpha kids come from multiracial and multicultural families, which also contributes to their diversity.

- Attention Span: Gen Alpha may have even shorter attention spans due to the constant access to the Internet and social media from a very young age due to the constant access to the Internet and social media from a very young age.
- Adaptability and Resilience: Gen Alpha has grown up in a world that is even more rapidly changing, so they may be even more adaptable and resilient. With technology and the Internet advancing at an even faster pace, as well as global events like the COVID-19 pandemic which have had a significant impact on the world, this rapid change may have resulted in Gen Alpha being more adaptable and resilient than Generation Z, as they have had to navigate a more rapidly changing world at a much younger, more impressionable age in their formative years.
- Environmentally Conscious: Gen Alpha is more environmentally aware, as they have grown up in a time when environmental issues are more pressing and more in the public consciousness. They are more understanding of climate change and the effect it is having on our world, so much so that many of them are actively taking steps to reduce their own carbon footprint and advocate for policies to address environmental issues.

  They are also more likely to make purchasing decisions based on a company's environmental practices.[46]

Activity

An activity may include the following topics for an ethics discussion. Using the scenarios for each, and the chapter content, discuss the decisions the students provide, including whether they want the action (decision) posted on social media for all to see.

Topic: Your parents provide you with a smartphone, and they disable browsing, social media sites, and the installation of apps. Your friends show you a way to work around these restrictions.

- What do you do? Obey your parents' restrictions? Install a site and post pictures, hoping they never find out?
- What are the ethical choices to be made?
- Do you want your posts and pictures seen by friends and family, and even people you don't know?

Topic: You're allowed to play specific games online during specific times, but you are not allowed to "chat" with any other players and not allowed to access any chat rooms. You receive a chat from someone who says you are a great player and wants to chat with you.

- What do you do? Obey your parents' restrictions or open a chat group and hope your parents never find out?
- What are the ethical choices to be made?

Topic: You catch your younger sibling chatting and exchanging pictures with someone they do not know personally but have met online. You know this is risky behavior.

- What do you do?
- Discuss the choices and ramifications of each.

In discussing ethics in business situations, the question often asked is "Do you want to see your decision and your action on the front page of the newspaper?" Although not a business decision and reading the newspaper is not a practice this generation knows, the question is still relevant: "Do you want your decision, and your action posted for everyone to see on social media?"

The MBA Research and Curriculum Center is dedicated to supporting educators in the preparation of students for careers in the areas of business management, finance, marketing, hospitality and tourism management, and entrepreneurship. Established in 1971, as a not-for-profit organization operated and governed by a consortium of state education departments.

Through the support of the Daniels Fund, a foundation in Denver, Colorado, supporting principle-based ethics, MBA Research provides free ethics education resources at the middle school, high school, and community college/postsecondary levels in schools across the nation.[47]

While discussing careers for seventh and eighth-grade students may seem a stretch for our discussion, providing support and guidance at this time will develop a solid foundation for their future and growth in advanced grades and beyond.

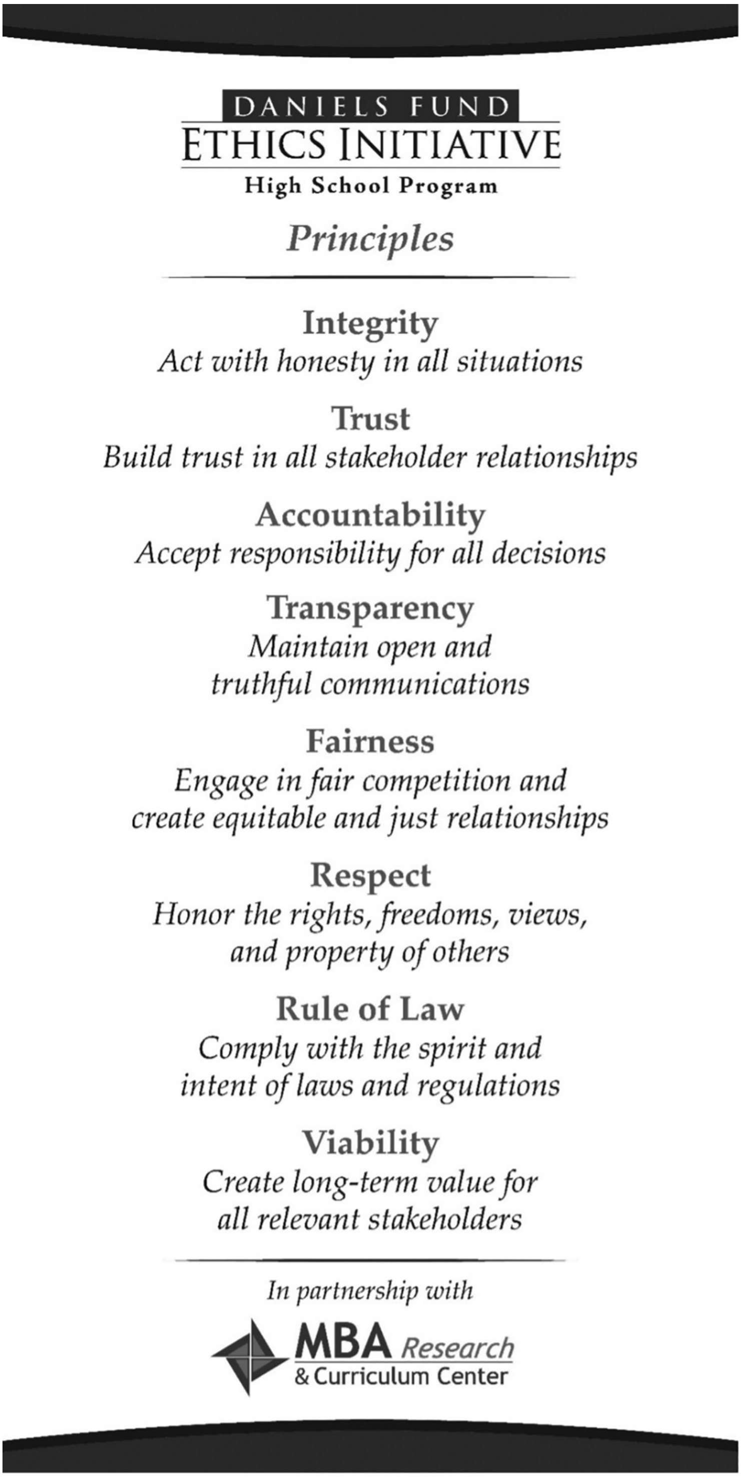
The Daniels Fund provides a list of Principles in its Ethics boot camp, which you may incorporate into your discussions (see Figure 1.9).

This figure shows a list of the ethics principles from the Daniels Fund, a foundation in Denver, Colorado, supporting principle-based ethics in schools. The principles are Integrity, Trust, Accountability, Transparency, Fairness, the Rule of Law, and Viability.

Thinking back to the discussion of good character at the beginning of this chapter, let's summarize character examples as follows:

- Understanding, caring about, and acting upon core ethical values
- The set of characteristics that motivate and enable one to function as a moral agent, do one's best work, effectively collaborate in the common space to promote the common good, and inquire about and pursue knowledge and truth
- A set of personal virtues that produce specific moral emotions, inform motivation, and guide conduct
- The traits and moral or ethical qualities are distinctive to an individual.[48]

Spend some time discussing the terms used in Figure 1.9 to ensure a common understanding and starting point for future discussion.



DANIELS FUND
ETHICS INITIATIVE
High School Program

Principles

Integrity
Act with honesty in all situations

Trust
Build trust in all stakeholder relationships

Accountability
Accept responsibility for all decisions

Transparency
Maintain open and
truthful communications

Fairness
Engage in fair competition and
create equitable and just relationships

Respect
Honor the rights, freedoms, views,
and property of others

Rule of Law
Comply with the spirit and
intent of laws and regulations

Viability
Create long-term value for
all relevant stakeholders

In partnership with

MBA Research
& Curriculum Center

Figure 1.9 Daniels Fund Ethics Initiative.[49]

Teaching Tip

Terms and definitions may include the following:

- Who is a stakeholder?
  A person involved in or affected by a course of action.
- What is integrity?
  Being honest and having strong moral principles; being incorruptible. Asking “What would you do if no one was looking?”
- What are morals?
  Standards of behavior regarding a belief in what is right and wrong.
- Is accountability different from responsibility?
  Responsibility speaks to what one needs to do; it’s about obligations and is task- or action-focused. Accountability is about owning what was done and the outcomes.
- What is the “spirit of the law”?
  The spirit of the law is often contrasted with the letter of the law. The spirit of the law is to follow the intention, or the purpose, of the law when written. The spirit of the law refers to the literal reading of the law without regard to why it was written.

Teachers and parents share responsibility in helping teens make good decisions. Where and how to start? Honor the teens’ independence by including them in decisions that directly impact them. It also must include being a sounding board, as they strengthen their capacity to think through decisions.

The Center for Parent and Teen Communication offers these tips for supporting teens in making wise decisions:

Promote Independence: Look for clues that students are ready to take on more responsibility. Give teens the space required to make decisions when possible, and gradually increase their independence as they demonstrate mature choices. Some of these clues include the ability to (a) think about future consequences of decisions and behaviors, (b) identify the pros and cons of different options, and (c) think before acting (i.e., have good “impulse control”).

Model Healthy Decision-Making: Talk through your thinking process when you are making decisions for yourself, so your students can understand the different aspects of making decisions. They are always watching and many learn best by viewing others.

Encourage Teens to Have a Voice: Think about how to seek out their opinions, concerns, and ideas. You might ask “What do you think about this?,” “What concerns do you have?,” or “What do you think we should do?” Even for major decisions for which you will have the “final say,” students can still have a voice. When they feel that they have a voice, they consider the decision-making process fairer.

Be Available: Be ready to provide guidance and support for decision-making when asked for it. Although we sometimes assume teens want to make decisions on their own, they typically want guidance for big decisions and are frustrated when they don't receive the support they need.

Plan Ahead: Help your students think ahead about scenarios in which decision-making might be more difficult, such as in stressful situations or when peers are present. These are times when teens may be more likely to act on emotion instead of thinking things through more carefully.[50]

It is important that children have stronger mentors and trusted adults to guide them. Feelings of isolation with no one to turn to and no guidance create bullying opportunities and can lead to poor choices. Children are now progressing to more frequent and advanced online activities, which are explored below and in subsequent chapters.

Artificial Intelligence

> For AI to serve everyone, it must understand everyone.
>
> — *Nell Watson*[51]

The following discussion provides the reader with a nontechnical overview of AI … a technology that has become both a bane and a benefit to educators since the debut of the most talked about, publicly available AI tool, ChatGPT.

What Is Artificial Intelligence?

The global AI market size was valued at USD 515.31 billion in 2023 and is projected to grow from USD 621.19 billion in 2024 to USD 2,740.46 billion by 2032, exhibiting a Compound Annual Growth Rate of 20.4% during the forecast period. North America dominated the global market with a share of 41.23% in 2023.[52]

One of the challenges with defining AI is that if you ask 10 different academics, data scientists, or industry practitioners, you will receive 12 different definitions. Defining AI is a moving target. The folks involved with AI today (which seems like almost everyone) haven't converged yet on exactly what a comprehensive, workable, acceptable definition is.

A consensus, however, not a definitive definition, is evolving among AI practitioners. For example…

John McCarthy, one of the founding figures in AI and the person who coined the term "Artificial Intelligence" in 1956, defined AI as "the science and engineering of making intelligent machines, especially intelligent computer programs."

Elaine Rich, a computer scientist and author of the book *Artificial Intelligence*, identifies AI as "the study of how to make computers do things at which, at the moment, people are better."

And finally…

According to Marvin Minsky, a cognitive scientist and one of the founding fathers of AI, "AI is the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions."

The common theme expressed by these scientists and industry practitioners is the concept of machines or computers exhibiting intelligent behavior similar to humans. The simulation of human intelligence underlines the idea of machines being programmed to think and act like humans.

Table 1.3 provides examples of common AI usage that an educator may elect to use when discussing the concept and application of current AI tools with seventh- and eighth-grade students.

What Is Generative AI?

Generative AI (GEN-AI) is a type of AI that can create new content, such as images, music, stories, and more, by learning from existing examples. Imagine it as a virtual

Table 1.3 Examples of Common AI Usage

AI USAGE — EXAMPLE	EXPLANATION OF AI APPLICATION
Autocorrect and predictive text	AI helps in correcting spelling mistakes and suggesting words or phrases while typing on smartphones or computers, improving communication efficiency.
Chatbots (e.g., customer service bots)	AI powers chatbots that can answer common questions, provide information, or help resolve issues online, simulating a conversation with a human.
Educational games (e.g., math apps)	AI can adapt to a student's learning level, providing personalized challenges and feedback in educational games, helping students learn at their own pace.
Facial recognition (e.g., smartphone unlock)	AI enables devices to recognize and verify a person's face for security purposes, such as unlocking phones or authorizing payments.
Self-driving cars	AI helps autonomous vehicles navigate roads, avoid obstacles, and follow traffic rules, with the goal of improving safety and convenience in transportation.
Smart recommendations (e.g., Netflix)	AI analyzes viewing habits and preferences to suggest movies and TV shows that a user might enjoy, making it easier to find content that matches their interests.
Social media feeds (e.g., Facebook, Instagram)	AI determines which posts to show in a user's feed based on their interests, likes, and interactions, ensuring relevant content is displayed.
Spam filters (e.g., email)	AI identifies and filters out unwanted or harmful emails, such as spam or phishing attempts, to protect users from potential threats.
Translation tools (e.g., Google Translate)	AI translates text or speech from one language to another, making it easier to communicate with people who speak different languages.
Voice assistants (e.g., Siri, Alexa)	AI powers these virtual assistants to understand and respond to voice commands, helping users set reminders, play music, or search the web without using their hands.

artist or writer that can generate new, original pieces based on what it has learned, much like how a human artist might create a new painting after studying many different styles and techniques.

For example, if you ask a generative AI to "draw a picture of a beach at sunset," it can create a unique image based on its understanding of beaches and sunsets from the many examples it has been trained on. This is different from just copying a picture it has seen before; instead, the AI combines elements from its training to produce something new.

When explaining this to your seventh- and eighth-grade students, you might say, "Generative AI is like a really smart computer that can create new pictures, stories, or music by learning from a lot of examples. It's a tool that helps you bring your ideas to life in a creative way."

The Growing Role of Generative AI in Education

Generative AI tools are increasingly being used by students, particularly in upper elementary and middle school grades. These tools offer several benefits that align well with educational goals, especially for students in seventh and eighth grades:

1. **Enhancing Creativity and Engagement:** Tools like DALL-E and MidJourney allow students to visualize their ideas in unique ways. For example, a student might use these tools to create artwork for a class project, helping to make learning more engaging and fun. By enabling students to see their creative ideas come to life, these tools foster a deeper connection to the material being studied.
2. **Personalized Learning:** AI tools like ChatGPT can offer personalized explanations and support, tailoring responses to match each student's learning style. This is especially useful in helping students grasp difficult concepts, as the AI can provide multiple explanations or break down complex ideas into simpler terms.
3. **Improving Writing and Communication Skills:** Writing tools powered by AI, such as Jasper AI and WriteSonic, can assist students in organizing their thoughts and generating content for assignments. These tools can help students improve their writing skills by offering suggestions and corrections, ultimately boosting their confidence and ability to communicate effectively.
4. **Making Learning Interactive:** Generative AI can turn abstract concepts into tangible learning experiences. For instance, students can use AI to simulate historical events or conduct virtual experiments in science. This makes subjects like history and science more interactive and easier to understand, helping students to engage with the material in a more meaningful way.
5. **Building Digital Literacy and Critical Thinking:** Early exposure to AI tools helps students develop essential digital literacy skills. By learning how to use these technologies creatively and responsibly, students are better prepared for

the future, both academically and in their eventual careers. They also develop critical thinking skills, as they learn to evaluate the outputs generated by AI and refine their prompts to get better results.

6. **Promoting Collaboration and Feedback:** Platforms like RunwayML and Artbreeder encourage collaborative projects where students can work together to create and enhance media. This not only fosters teamwork but also allows students to give and receive feedback, further enhancing the learning experience.

Table 1.4 provides the reader with a list of the top generative AI tools available on the market for general consumer use as of this writing. The GEN-AI tools are presented in order based on the popularity, usage, and installation base of each tool, reflecting their widespread adoption and influence in the consumer market.

Beyond their use and application in industry, these AI tools may certainly be used by educators in developing engaging class exercises and stimulating homework assignments for their students.

Educators may wish to explore each tool independently first, learning about the tool's features, application to the classroom, and engaging students. Then select specific tools to review together with students and explore uses and applications relevant to the students' objectives, assignments, and learning goals.

Table 1.4 Top Generative AI tools

GEN-AI TOOL NAME	DESCRIPTION	PRIMARY APPLICATION
ChatGPT	A conversational AI developed by OpenAI, capable of generating human-like text based on input prompts.	Chatbots, content creation, customer service
DALL-E	An image generation tool by OpenAI that creates images from textual descriptions.	Image generation for creative projects, design, and marketing
Jasper AI	A writing assistant that helps generate content such as blog posts, marketing copy, and social media posts.	Content creation, copywriting, marketing
MidJourney	A generative AI tool focused on creating visually stunning art based on text prompts.	Artistic creation, design, digital art
WriteSonic	An AI-powered writing tool that helps generate various types of written content.	Content creation, blog writing, marketing
Copy.ai	An AI tool for generating marketing copy, emails, and other business-related content.	Copywriting, email marketing, business communication
Synthesia	A video creation platform that uses AI to generate videos with realistic avatars and voiceovers.	Video production, training videos, personalized content
RunwayML	A platform that provides various AI tools for creators, including video editing, image generation, and text-to-image synthesis.	Video editing, creative projects, art generation
Artbreeder	A collaborative platform for creating and remixing images using generative AI.	Image generation, collaborative art projects

NOTE: Table 1.4 tools list is current as of 2024 manuscript submission.

The Impact of AI on Middle School Students and Academics

The Role of AI in Everyday Life

As AI technology becomes increasingly integrated into our daily lives, educators must assist middle school students in understanding its impact both inside and outside the classroom. Before diving into discussing the complexities of AI, it will be beneficial to begin discussions by having students identify the presence of technology in their everyday experiences.

By engaging students in conversations about the devices they use — such as smartphones, tablets, and computers — educators can build a foundation that makes it easier to introduce more complex AI concepts later on.

For instance, educators may start by asking their students how they use technology in their daily routines. From streaming music to using voice assistants like Siri or Alexa, these interactions with AI-driven tools are already shaping their lives. Educators can then guide students to recognize that AI is not just a futuristic concept but an active part of the world they live in today.

AI in the Classroom: Enhancing Learning Experiences

AI has the potential to revolutionize education by making learning more personalized, interactive, and engaging. The following examples provide insight into key areas where AI impacts academics at the middle school level.

1. Personalized Learning: AI-driven educational platforms like DreamBox and Khan Academy offer personalized learning experiences by adapting lessons to each student's pace and understanding. These platforms analyze a student's performance and provide tailored exercises that target specific areas of need, assisting students in mastering concepts at their own pace.
2. Interactive Learning: AI tools such as virtual tutors and interactive simulations allow students to engage with subjects in new ways. For example, AI-powered simulations in science classes can enable students to conduct virtual experiments, exploring concepts that might be too complex or dangerous to try in a traditional classroom setting.
3. Enhanced Feedback: Tools like Grammarly and automated essay scoring systems offer instant feedback on writing assignments, allowing students to improve their work in real time. This immediate feedback loop not only assists students in understanding their mistakes but also encourages them to revise and refine their writing, ultimately leading to better learning outcomes.
4. Supporting Diverse Learning Needs: AI technologies are particularly valuable in supporting students with diverse learning needs. For example, speech-to-text software and AI-powered reading assistants can help students

with learning disabilities access a course curriculum more effectively. These tools provide the opportunity for all students, regardless of their challenges, to succeed academically.

AI Beyond the Classroom: Preparing Students for the Future

The influence of AI extends beyond academic performance; it also plays a critical role in preparing students for the future. Below are examples of how AI is shaping the skill sets of middle school students.

1. Digital Literacy and Critical Thinking: Early exposure to AI tools helps students develop essential digital literacy skills. As they interact with AI, students learn to critically evaluate information, understand the ethical implications of technology, and make informed decisions about how to use these tools responsibly.
2. Creativity and Innovation: AI tools like DALL-E for image generation or WriteSonic for creative writing enable students to push the boundaries of their creativity. By experimenting with these tools, students learn to innovate and express their ideas in new and exciting ways.
3. Collaboration and Communication: AI-powered platforms that facilitate collaborative projects encourage students to work together, share ideas, and provide feedback. This collaborative environment mirrors the real-world workplaces where AI tools are increasingly used, helping students to develop teamwork and communication skills that will be invaluable in their future careers.

AI Challenges and Considerations for Educators

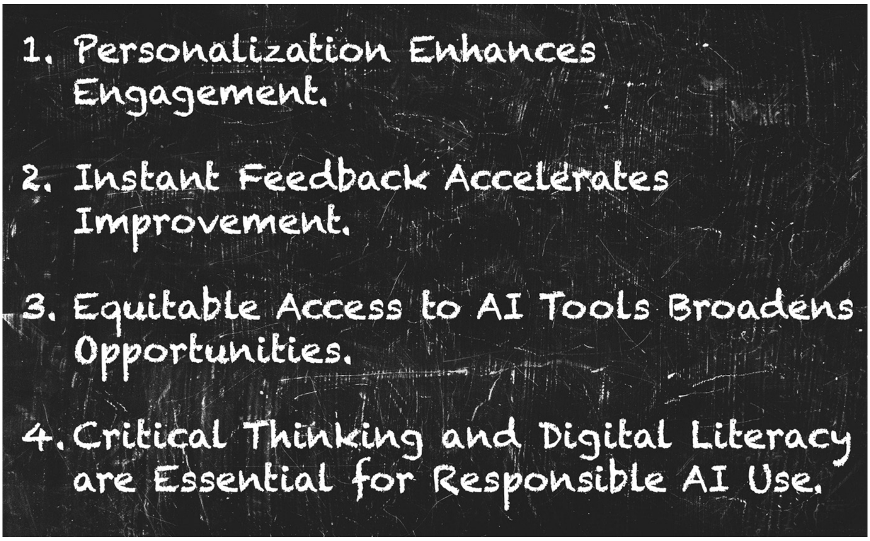
While the integration of AI into middle school education and curricula offers many benefits, AI also presents challenges that educators need to address.

1. Equity and Access: Ensuring that all students have access to AI tools is a significant challenge. Schools must work to provide equal access to technology so that no student is left behind due to a lack of technology or technological resources.
2. Teacher Training: Educators need adequate training to effectively incorporate AI tools into their teaching. Professional development programs that focus on AI literacy and the pedagogical use of AI can help teachers feel more confident in using these tools in the classroom.
3. Ethical Considerations: As AI becomes more prevalent, it's important to discuss the ethical implications with students. Educators should guide students in understanding issues such as data privacy, algorithmic bias, and the responsible use of AI technologies.

AI technology is not just reshaping the way students approach education and the overall learning process, but also preparing them for a future where these skills will be essential. By incorporating AI into middle school academics, educators can provide a more personalized, interactive, and equitable learning experience for their students.

However, it's crucial to approach this integration thoughtfully, ensuring that all students have access to the tools they need and that educators are well equipped to guide them in their AI journey. By doing so, we can help middle school students not only succeed academically but also thrive in an AI-driven world.

Four basic tenets of the impact of technology, specifically AI, on the academic learning of middle school students are presented (see Figure 1.10).



1. Personalization Enhances Engagement.
2. Instant Feedback Accelerates Improvement.
3. Equitable Access to AI Tools Broadens Opportunities.
4. Critical Thinking and Digital Literacy are Essential for Responsible AI Use.

Figure 1.10 AI usage in education: four tenets.[53]

Responsible AI (RAI)

RAI is a governance framework that defines the principles and practices an organization follows to address AI's societal, ethical, and legal impact. The framework calls for a human-centered approach to AI development that reflects the needs of a diverse set of users and cross-industry ethical standards.

GEN-AI is focused on the creation of man/machine intelligence and the ability to re-create human thoughts, actions, creativity, and output. RAI is focused on the consequences of this re-creation.

Responsible AI and Tech Justice

A key element is glaringly missing from conversations about the future of AI in education. While it is critical to delineate guidance for how teachers, students, and schools use AI tools in the advancement of education, it is equally important to prioritize how students and educators interrogate ethics, equity, and justice in the creation, deployment, and utilization of AI technologies as a core component of a robust K—12 education.

Responsible AI and Tech Justice is a robust and comprehensive course of study that utilizes an explicit racial and social justice lens to equip all students with the knowledge and resources to critically interrogate the ethical and equitable development, deployment, and impacts of AI, while simultaneously challenging, disrupting, and remedying the harms that these various technologies can cause within individual's lives, communities, and society at large.

The Kapor Foundation, through the development and release of *The Responsible AI and Tech Justice Guide for K—12 Education,* established six core components to serve as a guide for educators, parents, policymakers, and advocates seeking to design learning experiences across educational settings, where both the critical interrogation of technologies and the disruption and creation of more ethical and equitable solutions are prioritized.

The core components cover the large concepts and are complemented by a set of concepts, which provide suggested ideas to cover while allowing space for creativity, innovation, and content evolution as the space rapidly evolves.

The goal is that these six core components will be used by a range of K—12 educators, including teachers, instructional coaches, administrators, and curriculum providers, to inform their policies, practices, and resources directly.

These core principles are as follows:

1. Examine the AI technology creation ecosystem from who designs and develops products and how they are developed, to who invests in their creation and benefits from their adoption.
2. Interrogate the complex relationship between technology and human beings, including human–computer interaction and topics such as values, ethics, privacy, and safety.
3. Explore the impacts and implications of AI technologies on society, including positive benefits, negative consequences, and the perpetuation of exclusion, marginalization, and inequality.
4. Interrogate personal usage of AI technologies to become critical consumers of products and address misuse, exploitation, and safety concerns.
5. Build a critical lens in the collection, usage, analysis, interpretation, and reporting of data.
6. Minimize, mitigate, and eliminate harm and injustice caused by AI technologies through both the responsible and ethical creation process and the individual and collective right to refusal.

The Responsible AI and Tech Justice Guide for K—12 Education represents a first step toward incorporating principles of ethics, equity, and justice in the critical analysis of AI technologies within K—12 education and builds upon decades of critical scholarship and activism across disciplines ranging from computer science and machine learning (ML) to history, political science, and sociology.[54]

The Role of Leadership, Maturing AI, and Cyber Safety

Leadership plays a crucial role in setting the vision and strategy for integrating AI technologies in a way that enhances cyber safety. Leaders must understand the capabilities and limitations of AI to guide its implementation effectively.

As AI technologies mature, they become more sophisticated in detecting and responding to cyber threats. ML algorithms can analyze vast amounts of data to identify patterns and anomalies that might indicate a security breach.

Achieving long-term cyber safety is dependent on the innovative application of AI technologies, supported by leadership that encourages exploration and adaptation to new challenges.

Teaching Seventh- and Eighth-Grade Students the Value and Importance of Responsible AI

Teaching Tip

Educators may wish to incorporate this five-step process designed to open discussions with students on the value and importance of RAI. All material provided may be adjusted to meet student needs and time availability requirements.

Step 1: Introduction to AI

- Objective: Help students understand what AI is and how it impacts their daily lives.
- Activity: Begin with a brief discussion or video about AI, highlighting everyday examples like voice assistants, recommendation systems on streaming platforms, and smart devices. Ask students to share their experiences with AI.
- Key Point: AI is a powerful tool that makes many tasks easier and more efficient, but it must be used responsibly.

Step 2: Exploring AI's Potential and Risks

- Objective: Discuss the benefits and risks associated with AI.
- Activity: Divide the class into two groups. One group lists the positive impacts of AI (e.g., personalized learning, medical advancements), while the other group lists potential risks (e.g., privacy concerns, bias in AI decisions). Each group presents their findings.
- Key Point: While AI can greatly benefit society, it also poses risks that need to be managed carefully.

Step 3: The Ethics of AI

- Objective: Introduce the concept of AI ethics and why it's important.
- Activity: Present a simple scenario where AI makes a decision (e.g., an AI deciding who gets a loan). Ask students whether they think the decision was fair and why. Discuss concepts like bias, fairness, and transparency.
- Key Point: AI systems must be designed and used in ways that are fair, transparent, and respectful of everyone's rights.

Step 4: RAI Use

- Objective: Encourage students to think about how they can use AI responsibly.
- Activity: Give students a worksheet with different AI-related scenarios (e.g., using AI to generate schoolwork, or sharing personal data with AI services). Have them work in pairs to decide how they would responsibly handle each situation and discuss their reasoning with the class.
- Key Point: Being responsible with AI means making choices that are ethical, safe, and respectful of others.

Step 5: Reflection and Commitment

- Objective: Have students reflect on what they've learned and make a personal commitment to RAI use.
- Activity: Ask each student to write a short reflection on how they plan to use AI responsibly in their own lives. Then, have them share one commitment with the class (e.g., "I will think about the privacy settings on my apps" or "I will be careful not to rely too much on AI for my homework").
- Key Point: Everyone has a role to play in ensuring that AI is used in a way that benefits society and minimizes harm.

An Overview of AI Fundamentals

AI is part of the larger field of Data Science, which combines domain expertise, programming skills, and knowledge of mathematics and statistics to extract meaningful insights from data.

AI allows a silicon-based unit (i.e., a computer) to solve problems (and increasingly complex ones) that were originally solved by carbon-based lifeforms (i.e., humans). AI simulates human intelligence, at least that is the ultimate end game.

Spend any length of time reading about AI, and you will inevitably encounter two subsets of AI, Natural Language Processing (NLP) and ML.

NLP allows AI to read, interpret, and understand human language. NLP focuses on computer–human language interactions, specifically how to program computers to process and analyze large amounts of natural language data. The goal of NLP is for computers to eventually be able to recognize and process text and languages in the same way humans do.

ML as the name suggests, provides the basis for AI systems to learn and improve responses to queries through experience that does not require specific programming to further an ever-increasing level of intelligence. The goal is to find patterns within enormous amounts of data and make predictions based on those observed patterns. ML is primarily concerned with accuracy and pattern recognition.

A subset found within ML is Deep Learning (DL). DL is a method in AI that teaches computers to process data inspired by the human brain. DL models recognize complex patterns in pictures, text, sounds, and other data to produce accurate insights and predictions.

Finally, a subset of ML and at the heart of DL algorithms, we find neural networks, also known as Artificial Neural Networks (ANNs) or simulated neural networks. Their name and structure are inspired by the human brain, mimicking the biological neurons' signal to one another. Neural networks rely on training data to learn and improve their accuracy over time.

We use NLP and ML many times throughout the day, and many of us never realize it. When did you last ask Siri about traffic conditions before you headed out for your morning commute to work or Google Assistant to access information from your calendars and other personal information?

Often the best and most direct approach to explain a complex concept is through a picture. Under the umbrella of data science, Figure 1.11 shows the relationship between AI, NLP, ML, DL, and ANNs. It is important to note that AI is much more complex than shown. AI includes many other subdisciplines and techniques, a discussion of which is beyond the scope of this book.[55]

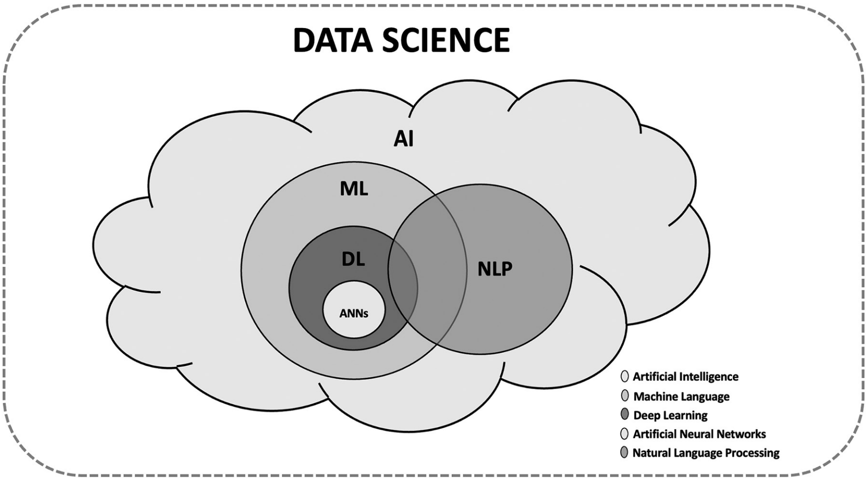


Figure 1.11 The relationship between AI, NLP, ML, DL, and ANNs.[56]

How Do AI Systems "Learn?"

Just like developing good characteristics in students throughout their educational journey, technology like AI must be taught to demonstrate good characteristics. AI systems that exhibit characteristics like resilience, integrity, reliability, security, robustness, interoperability, and privacy are exhibiting good characteristics. If AI systems are going to be trusted, useful, adopted, and accepted by people without fear, they must exhibit good characteristics and acceptable behavior.

Teaching AI systems to behave acceptably and embrace approved societal good behaviors and norms, like students, must be taught. Teaching AI systems is not too different than teaching students. In the classroom and through coaching, exercises, and lessons, students are presented with examples of desirable or good characteristics and acceptable behavior. These lessons are repeated throughout a student's academic experience.

Training AI Systems

Training AI systems involves a process similar to teaching a computer how to perform specific tasks or make decisions by exposing it to large amounts of data. This process is known as machine learning (ML). At its core, ML is the subset of AI that enables systems to learn and improve from experience without being explicitly programmed. The fundamental concept is to input millions if not billions of bytes of data that represent information into the AI system. This input or "feeding" process allows the AI system to recognize patterns, make predictions, or classify information autonomously.

One primary method of training AI is called supervised learning. In this approach, the AI system is provided with a labeled dataset, where each input is paired with the correct output. For instance, if we want the AI to identify pictures of cats and dogs, we will present the AI system with a collection of images labeled as either a cat or a dog. The AI learns by adjusting its internal parameters through repeated exposure to these labeled examples, refining its ability to make accurate predictions. Supervised learning is analogous to a teacher guiding a student with correct answers during a learning process.

Another key training method is unsupervised learning. Here, the AI explores data without explicit guidance, seeking to identify hidden patterns or relationships. Clustering, a common unsupervised learning technique, involves grouping similar data points. Imagine a scenario where the AI receives a mix of unlabeled pictures and independently discovers that some share characteristics, effectively categorizing them into groups. This unsupervised learning is comparable to a student independently organizing information based on inherent similarities.

Reinforcement learning is a third approach, inspired by behavioral psychology. In this method, the AI, often referred to as an agent, learns to make decisions by interacting with an environment. It receives feedback in the form of rewards or penalties based on the actions it takes. This trial-and-error process enables the AI to learn optimal strategies for maximizing rewards. Reinforcement learning can be compared to a student learning through experimentation and adjusting their behavior based on outcomes.

The training process also involves neural networks, which are computational models inspired by the human brain's structure. Neural networks consist of interconnected nodes (or artificial neurons) organized into layers. During training, the network adjusts the weights assigned to connections between nodes, optimizing its ability to make accurate predictions. The DL paradigm involves neural networks with many layers, allowing them to capture intricate features in the data. Visualize this as a student's brain adapting and strengthening connections as they acquire more knowledge and skills.

To summarize our review of AI and the various subsets that make up the broader field of AI, we are left with one elementary question… "How does artificial intelligence use data to make informed decisions?"

The answer is uncomplicated and straightforward … AI uses data to make informed decisions through a process called "machine learning." ML is a subset of AI that enables systems to learn from data, identify patterns, take actions, and make recommendations, predictions, or decisions based on that data (see Figure 1.12).

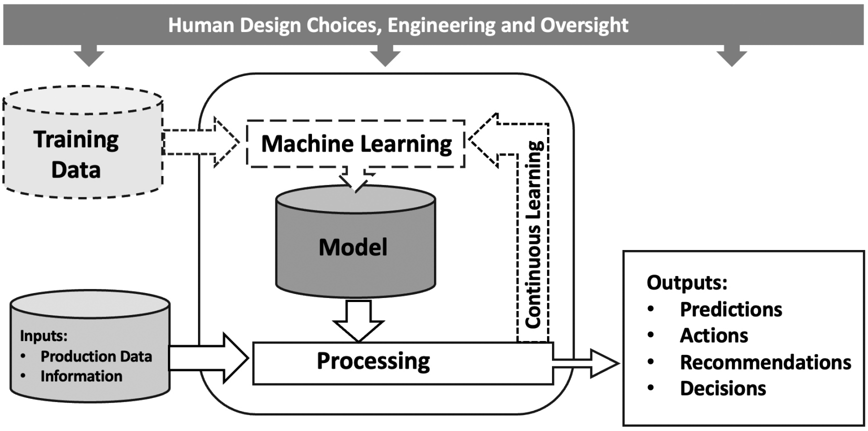

Human Design Choices, Engineering and Oversight
Training Data
Machine Learning
Model
Continuous Learning
Inputs:
• Production Data
• Information
Processing
Outputs:
• Predictions
• Actions
• Recommendations
• Decisions

Figure 1.12 AI functional overview.[57]

A Step-by-Step Approach to Training AI

The following stepwise approach simplifies the complex process of AI training. Educators may wish to incorporate this stepwise process into classroom discussions and exercises, making it easier for middle school students to grasp how AI learns and improves over time.

Step 1: Learning from Data

- Concept: AI learns by studying lots of examples, a process known as training.
- Explanation: Imagine you're trying to learn how to recognize different types of dogs. You would look at many pictures of dogs to understand their features. Similarly, AI learns by looking at a large amount of data, such as questions and answers, so it can understand how to respond correctly in the future.
- Application: Just as you learn about dogs by seeing many pictures, AI learns how to answer questions by examining many examples of question-and-answer pairs.

Step 2: The Training Process

- Concept: AI uses a vast collection of data called a dataset during its training.
- Explanation: During training, AI is given a dataset that includes pairs of questions and their correct answers. By studying these pairs, AI begins to recognize patterns and understand how to match questions with the right answers.
- Application: Think of this like a big book where each page has a question on one side and the correct answer on the other. AI reads this book many times to learn how to answer questions correctly.

Step 3: Practice and Feedback

- Concept: AI practices by answering new questions and then is given feedback on its accuracy.

- Explanation: After studying, AI practices by trying to answer new questions. If it gets an answer wrong, it receives feedback to help it understand what went wrong, allowing it to improve.
- Application: This is similar to doing practice quizzes at school. When your student gets a question wrong, you explain the correct answer so that the student can understand and do better next time. AI learns in the same way through feedback.

Step 4: Using Algorithms

- Concept: AI uses special rules and calculations known as algorithms to find patterns in the data.
- Explanation: AI applies algorithms to the data it has studied. These algorithms are like step-by-step instructions that help the AI determine the best way to respond to different questions based on the patterns that it has learned.
- Application: Imagine following a recipe to bake cookies. The recipe provides specific steps to ensure the cookies turn out right. Similarly, algorithms guide the AI to find the right answers.

Step 5: Continuous Learning

- Concept: AI continues to improve by learning from new data and feedback over time.
- Explanation: Even after AI starts giving answers, it keeps learning from new experiences. It gathers more data and feedback to refine its responses, becoming more accurate and effective.
- Application: As an example for your students, ask them to think of how they get better at a sport or playing an instrument the more they practice. AI is similar, it keeps practicing and learning from its mistakes, which helps it become better at answering questions (see Figure 1.13).

DATA
DATA
DATA
DATA

Figure 1.13 Training AI.[58]

Training AI By Example

AI learns to provide answers much like students learn in school. It starts with a lot of examples, practices with feedback, and improves over time by learning from its mistakes. The AI training process outlined below will better assist your students in understanding just how an AI application can process input data and provide an answer.

Teaching Tip

Step 1: Learning from Data (Collecting Examples)

- Explanation: Imagine you want to teach AI how to recognize different animals, like cats and dogs. One begins by showing the AI tool thousands of pictures of cats and dogs. The AI studies these pictures just like your students might study flashcards before a test.
- Student Resonance: Compare this to how students might study by looking at different types of math problems before a test. They look at many examples to understand the patterns.

Step 2: Training Process (Studying and Matching)

- Explanation: The AI is shown a picture of a cat with the label "cat" and a picture of a dog with the label "dog." It starts learning the differences between cats and dogs by comparing lots of these labeled pictures.
- Student Resonance: This is like when students match words with definitions in a vocabulary quiz. The more they practice, the better they get at matching the correct word to its definition.

Step 3: Practice and Feedback (Improving through Mistakes)

- Explanation: After studying, the AI starts practicing by trying to guess whether a new picture is a cat or a dog. If it guesses wrong, it gets corrected and learns from the mistake.
- Student Resonance: Relate this to taking a practice quiz in school. If students answer a question incorrectly, their teacher explains why, and they learn the right answer for next time.

Step 4: Using Algorithms (Following Rules to Find Patterns)

- Explanation: The AI uses algorithms, which are like rules or recipes, to figure out what makes a cat a cat and what makes a dog a dog. These rules help the AI decide based on the patterns it has learned.
- Student Resonance: Compare this to following a recipe to bake cookies. Just as a recipe tells students step-by-step how to make cookies, the algorithms guide the AI to figure out which animal is in the picture.

Step 5: Continuous Learning (Getting Better Over Time)

- Explanation: Even after the AI is good at recognizing cats and dogs, it keeps learning by seeing more pictures and getting feedback. This helps it get even better over time.
- Student Resonance: This is like when students continue to practice a sport or a musical instrument. The more they practice, the better they get, even after they've already learned the basics.

AI Risks: Praemonitus, Praemunitus![III]

Algorithms and AI tools have contributed to increased polarization, the proliferation of mis/disinformation, increased online safety and privacy concerns, and mental health challenges among teens and young adults. The massive amount of energy needed to power AI technologies can impact carbon emissions at a time when climate change is a leading global concern.[59]

One risk associated with GEN-AI is exactly what makes GEN-AI "intelligent," the use of excessively large amounts of data. Data can come from both known (substantiated) and unknown (unsubstantiated) sources.

Due to the vast amounts of data that GEN-AI models have access to, the ability for the generation, either intentional or unintentional, of harmful content is highly probable. Content that may inaccurately attribute comments to someone who never made the statement or alter images to deceive the viewer into believing that the image represents an authentic scene, person, or event.

In the field of AI and ML, this is referred to as hallucination. The production of plausible-seeming but factually incorrect output by a generative AI model that purports to be asserting the real world, however, the AI system provides an answer that is factually incorrect, irrelevant, or nonsensical, because of limitations in its training data and architecture.

The potential for GEN-AI models to increase efficiency and productivity, make better decisions, improve the "speed" of business, reduce human error, and improve services comes with ethical concerns and risk exposures inherent in AI technologies and GEN-AI models … accountability and transparency, the potential to create and to distribute harmful content, privacy exposure, loss of data protection, trust and explainability concerns, job displacement, unemployment, and economic disruption, and data biases.

Throughout their academic journey, students learn about being an ethical person, and that responsibility and trust represent good characteristics and acceptable behavior. These lessons need to be reinforced and discussed with students in terms related to the world of technology. This is even more important now with the advent and presence of AI as a tool, a resource gaining increasing popularity in all sectors of society, including academia, and the increasing availability for student access and use.

Just as students learn what ethical and responsible behavior is, that trust is earned, how to trust, and that not everyone can be trusted, students must be provided with instruction and guidance on using AI ethically, and responsibly and that AI cannot always be trusted (meaning that AI, as it exists currently, will not always provide the correct answer).

[III] Forewarned is forearmed!

AI Hallucinations

The fact that AI cannot and does not provide a correct response 100% of the time (yet) has resulted in the introduction of a new term to our social lexicon … Hallucinations, specifically AI Hallucinations.

In the constantly evolving field of AI, hallucinations are incorrect or misleading results that AI models generate. These errors can be caused by a variety of factors, including insufficient training data, incorrect assumptions made by the model, or biases in the data used to train the model. AI hallucinations can be a problem for AI systems that are used to make important decisions, such as medical diagnoses or financial trading.

AI models are trained on data, and they learn to make predictions by finding patterns in the data. However, if the training data is incomplete or biased, the AI model may learn incorrect patterns. This can lead to the AI model making incorrect predictions or hallucinating.

AI hallucinations can take many different forms. Some common examples are as follows:

- False Positives: When working with an AI model, it may identify something as being a threat when it is not, for example, an AI model that is used to detect fraud may flag a transaction as fraudulent when it is not.
- False Negatives: An AI model may fail to identify something as being a threat when it is, for example, an AI model that is used to detect cancer may fail to identify a cancerous tumor.[60]

Unethical Uses of AI

> In the dance of progress, carbon and silicon must move in step. Co-adaptation ensures that the intelligence we create serves as an extension of our humanity, rather than a replacement.
>
> — *Fei-Fei Li, Co-Director of the Stanford Human-Centered AI Institute*

The ramifications of the unethical use of AI are numerous, and as AI matures, the list of potential consequences and risks of unethical AI grows as well (see Figure 1.14).

Currently, the most significant risks associated with the unethical use of AI are:

- Privacy Erosion: The unethical use of AI poses a significant threat to privacy. As AI systems gather and analyze vast amounts of personal data, there is a risk of unauthorized access, data breaches, and misuse.
- Bias and Discrimination: Unethical AI practices can perpetuate and even exacerbate societal biases. If the training data used to develop AI algorithms contains biases, the AI systems may produce discriminatory outcomes.
- Security Threats: The unethical use of AI can introduce new security threats, as malicious actors leverage AI to enhance the sophistication of cyberattacks.

- Job Displacement and Economic Inequality: The deployment of AI in the workforce, without ethical considerations, can lead to job displacement and economic inequality.
- Autonomous Weapons and Warfare: The unethical use of AI in developing autonomous weapons raises profound ethical and humanitarian concerns.
- Deepfakes are a form of AI used to create convincing images, audio, and video hoaxes. The term describes both the technology and the resulting bogus content and is a hybrid of DL and fake information. The greatest danger posed by deepfakes is their ability to spread false information that appears to come from trusted sources.[61]

  The widening availability of AI image generators, including some with few restrictions on their use, has led to an uptick in Nonconsensual Explicit Imagery, according to victims' advocates. The tools have made it easy for just about anyone to create spoofed explicit images of any individual, whether that's a middle school classmate or a mega-celebrity.[62]
- Persuasive AI refers to technology, like robots or computers, that is designed to influence or convince people to think or act in certain ways through words, images, or actions.
- Inequality in the context of unethical uses of AI refers to the unjust and disproportionate distribution of benefits, opportunities, or resources among individuals or groups due to biased algorithms, discriminatory practices, or unequal access to AI-driven technologies.

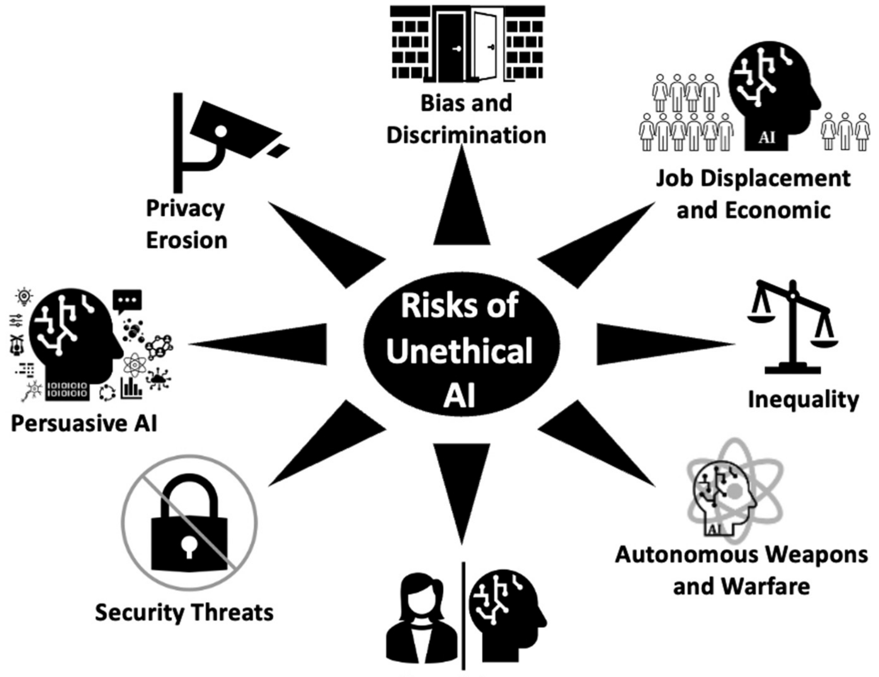

Bias and Discrimination
Job Displacement and Economic
AI
Privacy Erosion
Risks of Unethical AI
Persuasive AI
Inequality
Autonomous Weapons and Warfare
Security Threats
Deepfakes

Figure 1.14 Risks of unethical AI.[63]

Addressing the most significant issues of unethical AI requires a global recognition of the risks that can be inherent within AI and an effort to establish ethical frameworks, regulations, education programs, and RAI practices.

The Ethical Use of AI

AI will have a significant impact on the world in which our students live, learn, work, and grow. Teaching students to use AI ethically and responsibly is preparing them to manage AI as adults and use AI to build a safer, better world.

Just as there are risks when AI is used in an unethical manner, when used ethically, AI has global socioeconomic benefits (see Figure 1.15).

- Improved Healthcare: AI can help doctors diagnose diseases earlier and more accurately, leading to better treatment outcomes. It also assists in drug discovery, making treatments available faster.
- Enhanced Education: AI-powered tools can provide personalized learning experiences, helping students understand subjects better and allowing teachers to focus on individual needs.
- Increased Access to Information: AI makes it easier for people to access information quickly through search engines, virtual assistants, and translation tools, breaking down language barriers.
- Efficient Transportation: AI is used in traffic management and navigation systems, helping reduce travel time, fuel consumption, and traffic accidents.
- Job Automation: While AI can automate repetitive tasks, it also creates new job opportunities in emerging fields, allowing people to focus on more creative and meaningful work.
- Improved Customer Service: AI chatbots and virtual assistants are available 24/7, providing quick answers to customer inquiries, improving service quality, and saving time.
- Energy Efficiency: AI helps optimize energy use in homes and industries, reducing costs and minimizing environmental impact.
- Disaster Response and Management: AI can analyze data to predict natural disasters, assist in rescue operations, and manage resources during emergencies, potentially saving lives.

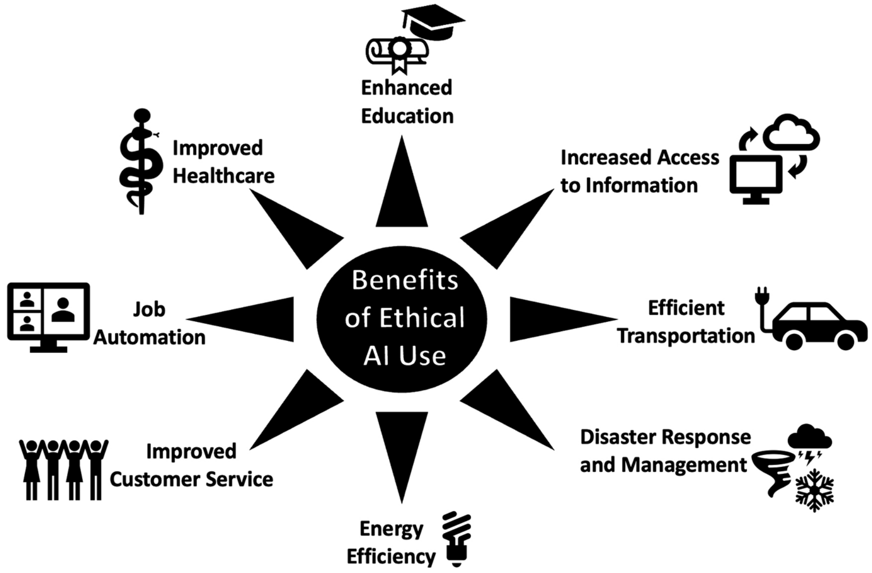

Enhanced Education
Improved Healthcare
Increased Access to Information
Benefits of Ethical AI Use
Job Automation
Efficient Transportation
Improved Customer Service
Disaster Response and Management
Energy Efficiency

Figure 1.15 Benefits of ethical AI use.[64]

Teaching students about ethical behavior and behaving responsibly can at times be challenging. For educators, applying these life skills to AI adds to this challenge. As AI becomes a bigger part of our lives, students need to understand how to use AI responsibly and ethically. This means using AI in ways that are fair, respectful, and safe.

Educators may wish to incorporate the following key concepts, discussion points, and activities into class discussions and exercises on good character, ethics, and the ethical use of AI.

The Ethical Use of AI: Classroom Discussion and Exercise

In attempting to teach middle school students both ethics and AI, educators often can identify teaching aids that excel in either ethics or AI, however, not so when attempting to combine both disciplines. The following material is provided for educators seeking to create in-class discussion lessons and group exercises, focused on reinforcing student learning in the concepts supporting and practicing ethical AI.

Teaching Tip

Objective:

Help students understand the importance of using AI responsibly and ethically.

1. Introduction to AI Ethics

   Concept: Explain that ethics are rules that help us decide what is right and wrong. When we use AI, it's important to think about these rules to make sure we're using technology in a way that is fair and doesn't harm others.

Teaching Example: Imagine if AI was used in a video game to always make one player win, no matter what. That wouldn't be fair, right? Just like in games, AI needs to be used in ways that are fair to everyone.

2. Privacy and Data Protection

   Concept: Teach students that AI often uses data to work. This data can include personal information like names, pictures, or even what websites they visit. This information must be kept safe and private.

   Teaching Example: Talk about social media. If an AI is used to suggest friends or ads, it's using information about what they like and who they talk to. This information mustn't be shared without permission. Ask them how they would feel if someone shared their secrets without asking — AI should respect privacy just like that.

3. Avoiding Bias in AI

   Concept: Explain that AI can sometimes make decisions that are unfair or biased if it's not taught correctly. This happens when the AI is only trained with one type of data, leading it to make unfair decisions about people or things it doesn't know well.

   Teaching Example: Ask the students to imagine a classroom where the teacher only gives good grades to students who wear glasses, because the teacher only learned that glasses make students smart. Then, discuss how this would be unfair to students who don't wear glasses, even if they are smart too. Explain that similarly, AI can make biased decisions if it's only trained on one type of data, which is why it's important to teach AI with diverse examples to ensure fairness.

4. Transparency and Understanding AI Decisions

   Concept: Students should understand that when AI makes decisions, those decisions should be easy to understand. Transparency means that we should be able to ask and know why the AI made a certain decision.

   Teaching Example: If a popular streaming service suggests that you should watch a certain movie, it should be clear why it made that suggestion. Was it because you liked a similar movie before? Was it because of the actors or actresses? The movie's soundtrack? Ask students how they would feel if an AI recommended something completely random without explaining why. They should understand that AI should be clear and logical in its actions.

5. Responsible Use of AI in Daily Life

   Concept: Discuss the importance of using AI responsibly, especially in daily activities like social media, school projects, and online interactions.

   Example: Ask students about using AI tools like spell checkers or calculators. It's okay to use these tools to help with schoolwork, but it's also important to learn and understand the material on their own. Discuss the balance between using AI to help and not letting it do all the thinking for them.

Activity: AI Ethics Role-Play

Objective:
Engage students in role-playing scenarios where they have to make decisions about using AI. This helps them think through ethical dilemmas in a fun and interactive way.

Example Scenarios:

- AI in Social Media: A friend uses an AI app to create fake photos of other students. Discuss whether this is fair or responsible and what could happen as a result.
- AI in Schoolwork: You're using an AI tool that writes essays. Should you let it write the entire essay, or should you use it to help you brainstorm ideas?
- AI in Games: A new game uses AI to learn your playing style and gets harder over time. Is it okay if the AI cheats to make sure you never win? Why or why not?

Encourage students to always think about how they use AI. Ask them to consider if their use of AI is fair, respectful of privacy, and responsible. Remind them that just because they can use AI to do something doesn't always mean they should — using AI wisely and ethically is important for everyone.

High-Level Machine Intelligence (HLMI)

HLMI refers to a form of AI that can perform most tasks that are economically relevant and require human intelligence, at or above the level of an average human. HLMI would be capable of autonomously solving complex problems across a wide range of domains, potentially matching or exceeding human performance in tasks such as reasoning, decision-making, language understanding, and perception.

Achieving HLMI is considered a significant milestone in AI development, often associated with concerns about the broader implications for society, ethics, and employment. As a global society, far too few people truly understand the range of applications of AI and its potential risks.

A 2022 survey of 559 AI and ML researchers conducted by AI Impacts asked respondents their beliefs about progress in AI … achieving high- or human-level machine intelligence. Results from this survey shed an interesting light on a future dominated by an increase in the presence and influence of AI.

Survey respondents indicated the following:

- The aggregate forecast time to a 50% chance of achieving HLMI was 37 years, i.e., 2059.
- The median respondent[IV] believed the following:

[IV] Median values are presented as these provide a better sense of the "typical" value because extreme values do not influence it.

- The probability is that the long-run effect of advanced AI on humanity will be "extremely bad (e.g., human extinction)."
- Society should prioritize AI safety research "more" than currently prioritized.
- There is an "about even chance" that a stated argument for an intelligence explosion is broadly correct.

Figure 1.16 represents the distribution of opinions (average responses from 559 ML experts) regarding the impact on humanity of achieving "high-level machine intelligence" when unaided machines can accomplish every task better and more cheaply than human workers.[65]

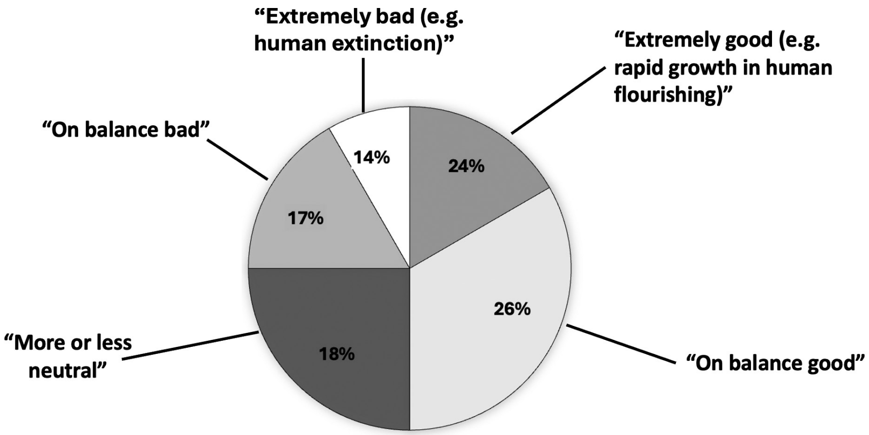


Figure 1.16 The overall impact of achieving HLMI on humanity.[66]

genAI[V] Literacy: An Important Goal for Surviving Our Collective Future

The risks inherent within AI are tempered by the promise of transformational new opportunities, such as accelerating drug development and scientific breakthroughs, improving clinical outcomes, optimizing infrastructure, assisting with crucial sustainability issues, and so much more.

In a world increasingly influenced and shaped by AI, acquiring and mastering AI literacy is no longer optional but necessary.

[V] The terms "GEN-AI" and "genAI" are often used interchangeably to refer to generative artificial intelligence, but there is a subtle difference based on context or usage. "GEN-AI" implies a broader system, encompassing various aspects of AI and generative processes, emphasizing the "AI" (Artificial Intelligence) technology part. The term "genAI" is introduced and used here to focus more on the generative aspect, highlighting AI's ability to create content, such as text, images, or music. genAI is also often used in developer or user communities where the emphasis is on the functionality and innovation of AI.

genAI Literacy refers to the knowledge and skills required to understand, effectively use, and critically evaluate generative AI (genAI) systems.

This includes comprehending how genAI models, such as those used in text, image, or code generation, function, the ethical implications of their use, and the potential biases and limitations inherent in these technologies. genAI literacy enables individuals to interact with AI-generated content responsibly, make informed decisions about its applications, and contribute to discussions about the societal impact of generative AI.

AI literacy empowers individuals to be informed decision-makers and benefits us all by preparing individuals to meaningfully engage in conversations about responsible and ethical development and the use of AI.

> Responsibly integrating genAI literacy and adopting the technology in K—12 education is the obligation of all stakeholders: parents, teachers, administrators, philanthropists, and policymakers.
>
> *Andrew Buher, Founder and Managing Director of Opportunity Labs*

To put a fine point on it … genAI literacy involves having the skills and competencies to use AI technologies and applications effectively.

genAI Literacy: A Foundation

As Matt Crabtree writes in his blog, genAI literacy is built on three fundamental understandings of AI … technical, practical, and ethical.[67] Parsing these fundamental understandings into concepts that an educator may use to engage students in the importance of attaining a level of genAI literacy, we can use terms a tad bit more friendly and understandable to students.

genAI consists of three core elements: technical comprehension, practical appreciation, and ethical awareness.

The first element is an in-depth understanding of the technology. This involves having a solid understanding of the fundamental principles of AI, including how AI perceives, collects, and processes data to make decisions or recommendations. It encompasses knowledge of AI's function or operating capabilities, like pattern recognition, ML, and NLP, as well as an awareness of AI's limitations. Limitations include understanding that AI's effectiveness depends on the quantity and quality of the training data used to "educate" the AI tool and that AI is not infallible and can be prone to errors, biases, and could be flat-out wrong, producing a completely inaccurate response.

Becoming more genAI literate will require society to approach AI more practically. This evolution in the growth of our genAI literacy involves understanding how to effectively interact with and use AI systems and recognizing their practical applications as well as their limitations.

This includes the ability to identify and use AI tools for such tasks as data analysis, transportation modeling, weather forecasting, risk modeling, human resource management, medical diagnosis, ESG sustainability and governance monitoring, banking & financial services, healthcare, and travel & hospitality and countless other applications.

A growth in genAI literacy will require an ability to construct meaningful as well as targeted prompts. Crafting a well-thought-out prompt is crucial when working with generative AI because it directly influences the quality and relevance of the output you receive.

Think of it like giving instructions: If your instructions are vague or incomplete, the result might not be what you intended. A well-crafted prompt helps the AI focus on the right details, reduces misunderstandings, and ultimately saves you time by minimizing the need for revisions or repeated queries. The better your prompt, the better the AI can assist you.

Lastly, but equally important (if not more so) is an understanding that AI has broad societal impacts. The effects of bad data and poor data cleansing processes raise considerable ethical issues associated with data biases, discrimination arising from those biases, further erosion of individual privacy, and the potential for the misuse of AI, including the genuine outcome of incorrect AI responses based on those data and learning model training methods (see Figure 1.17).

> AI is not always correct, nor is it values-neutral. All generative AI, by virtue of the fact that the models are trained on massive amounts of internet data, host a wide variety of cultural, racial, socioeconomic, historical, and gender biases.
>
> — *Tracy Pizzo-Frey, Senior Advisor of AI at Common Sense Media*[68]

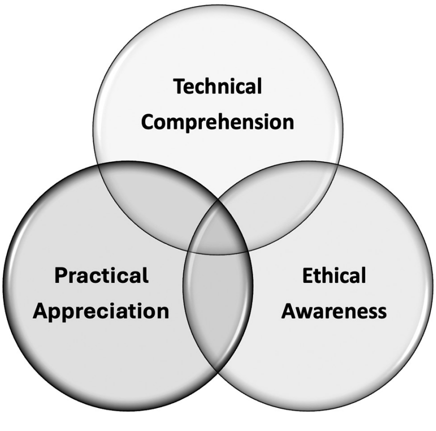


Figure 1.17 Foundation of genAI literacy.[69]

genAI Literacy: An Educational Process

Providing timely and constructive education to middle school students on developing, attaining, and maintaining genAI literacy can prove challenging. The technology, applications, and growth of the AI market are changing rapidly.

To effectively teach middle school students about the importance of developing, attaining, and maintaining genAI literacy, educators may wish to use the following approach that emphasizes relevance, engagement, and real-world applications.

1. Start with What They Know:

   Approach: Begin by discussing AI in the context of technologies they are already familiar with. This helps bridge the gap between their existing knowledge and the new concepts of genAI literacy.

   Example: Ask the students if they use voice assistants like Siri or Google Assistant. Explain how these tools use AI to understand and respond to their questions. Discuss how understanding AI can help them use these tools more effectively and responsibly.
2. Make It Interactive and Hands-On:

   Approach: Incorporate interactive activities that allow students to experience AI firsthand.

   Example: Use a simple AI tool or app that allows students to create their own AI-generated art or music. Discuss how the AI works behind the scenes and how understanding these processes can empower them to create even better content.
3. Connect to Real-World Scenarios:

   Approach: Illustrate the importance of AI literacy by connecting it to real-world scenarios that impact their lives or future careers.

   Example: Discuss how AI is used in gaming to create smarter, more challenging opponents. Explain that by understanding AI, they could potentially design better games or even pursue careers in game development.
4. Emphasize the Future Impact:

   Approach: Help students see the long-term benefits of AI literacy in terms of career opportunities and societal impact.

   Example: Talk about how AI is used in medicine to diagnose diseases or in environmental science to predict climate change. Encourage students to think about how they could contribute to these fields by understanding and developing AI technologies.
5. Encourage Critical Thinking:

   Approach: Foster a mindset of questioning and exploring the ethical implications of AI.

Example: Pose a scenario where AI is used in social media to recommend content. Ask students to discuss the benefits and potential downsides of this, such as privacy concerns or the spread of misinformation. This encourages them to think critically about how AI affects society and their personal lives.

6. Use Storytelling and Relatable Characters:

   Approach: Use stories or case studies that involve characters or situations students can relate to.

   Example: Create a story about a character their age who uses AI to solve a problem in their community, such as designing an app that helps local businesses or creating an AI-powered recycling program at school. This can inspire students to see themselves as capable of leveraging AI for positive change.

7. Incorporate Cross-Disciplinary Learning:

   Approach: Tie AI literacy into subjects they are already studying, such as math, science, or social studies.

   Example: In a science class, discuss how AI is used in space exploration or biology. In a math class, show how algorithms are created using mathematical principles, making AI tangible and relevant to what they are learning.

8. Create an Ongoing Conversation:

   Approach: Make AI literacy an ongoing topic in the classroom, revisiting it in different contexts throughout the year.

   Example: Start a classroom blog or discussion board where students can post articles or videos they find about AI. Encourage them to share their thoughts and questions, fostering a continuous and evolving understanding of AI literacy.

Using this process, educators can assist students in understanding the necessity of developing, attaining, and maintaining genAI literacy and help them better prepare to navigate and shape the AI-infused world they will grow up in.

AI Literacy for Educators

> To develop teachers' competencies to adapt AI-driven teaching and learning tools and approaches, educators need to timely update their skills and knowledge to create suitable learning environments for their students.[70]

Obtaining and sustaining literacy in AI is no longer an option for educators but a necessity. This literacy need not be into the depths of ML or algorithm design but to the level of proficiency to lead discussions on the topic and to design academic learning activities for students.

This level of proficiency should be a working knowledge of basic AI concepts and applications. Keeping abreast of the changes and advances in AI is part of an educator's continuing professional development.

Obtaining a deeper understanding of AI will allow the educator to investigate new pedagogical applications for teaching even the most fundamental courses, provide customized education and lessons, tailored to individual student learning needs and levels, and enhance and expedite assessment of student learning, allowing the educator to spend more time in the classroom teaching and interacting with students. Learning more about AI will also assist educators in protecting students and themselves through the knowledge of the risks associated with this technology and being better prepared to stay cyber-safe.

There are many options to learn more about AI (free and paid) available to educators, from self-study courses to traditional academic programs offered either in-person or virtually. Before venturing down this path, it is best to first evaluate your current knowledge of and comfort level with AI. If you can spell AI and have a beginning level exposure, starting with an entry-level AI 101 course is a logical option. As your knowledge and comfort level increase, moving on to courses that investigate the more technical aspects of AI will be a natural progression.

Ongoing research is being conducted on what AI competencies an educator should possess, as this technology is now a mainstay in the academic classroom. A set of teachers' AI competencies from this initial research suggests educators…

- Learn to use and incorporate basic IT applications in designing and presenting academic instruction.
- Manage and analyze information, and use data analytics software.
- Create engaging learning content using AI tools (see a list of such tools in this chapter).
- Connect students to technology.
- Integrate new digital technologies into daily lesson plans, in-class exercises, and take-home assignments.
- Support educational standards through the integration of digital technologies into all aspects of academic instruction.
- Engage in continual professional education and learning to build technical competencies.
- Gain experience using AI-enabled tools.
- Use adaptive learning systems and intelligent agents to facilitate daily teaching.
- Enhance personalized learning to understand students' learning progress and needs.
- Promote online collaboration among student learners, utilizing AI-enhanced software.
- Update personal/individual pedagogical and content knowledge on general AI topics, tools, and advances.

- Learn how to develop suitable pedagogies (e.g., collaborative learning, problem-based learning) and digital resources.
- Develop learning materials and assessments supported by AI tools to empower students.

To acquire these AI skills, Table 1.5 provides a general list of AI education programs. These programs were culled from the Internet and are representative. This list is not

Table 1.5 AI Literacy Programs for Educators

COURSE/PROGRAM NAME	ORGANIZATION/INSTITUTION	FREE/TUITION	MODE
AI and machine learning for business	Wharton School, UPenn	Paid	Virtual
AI applications with Watson	IBM (via edX)	Free/Paid (for certificate)	Virtual
AI developer professional certificate	IBM (via Coursera)	Free (with Coursera account)	Virtual
AI essentials for business	Harvard Business School	Paid	Virtual
AI for business	University of Pennsylvania	Paid	Virtual
AI for everyone	DeepLearning.AI	Free/Paid (for certificate)	Virtual
AI for social good	University of Oxford	Paid	Virtual
AI fundamentals	DataCamp	Paid	Virtual
AI in healthcare	Stanford School of Medicine	Paid	Virtual/In-person
AI strategy and implementation	Northwestern University	Paid	Virtual
Artificial intelligence & machine learning bootcamp	Caltech CTME	Paid	Virtual
Artificial intelligence: business strategies and applications	Berkeley Executive Education	Paid	In-person
AWS generative AI developer kit	Amazon Web Services (AWS)	Paid	Virtual
ChatGPT for beginners	GreatLearning	Free	Virtual
Designing and building AI products and services	MIT xPRO	Paid	Virtual
Elements of AI	University of Helsinki	Free	Virtual
Introduction to artificial intelligence	Stanford University (via Udacity)	Free	Virtual
Introduction to generative AI	Google Cloud	Free	Virtual
Jetson AI Certification	NVIDIA	Free	Virtual
Machine learning	Stanford University (via Coursera)	Paid	Virtual
Microsoft certified: Azure AI engineer associate	Microsoft	Paid	Virtual
Postgraduate program in AI and machine learning	Purdue University/IBM	Paid	Virtual
Professional certificate in machine learning and AI	UC Berkeley	Paid	Virtual
Professional machine learning engineer certification	Google Cloud	Paid	Virtual
S50's introduction to artificial intelligence with python	Harvard University	Free (with optional paid cert)	Virtual

an exhaustive list of the breadth and depth of such courses available to educators. The reader is advised to fully investigate and research any training program before committing financial resources and registering for any program.

One-Year Education Plan of Study: AI Literacy for Educators

The following is an example/a proposed one-year education plan for an educator teaching at the primary to middle school level interested in obtaining a basic but solid understanding and literacy of AI. Each quarter focuses on specific areas of AI, building knowledge progressively. This proposed course of study is *NOT* a degree program or one that leads to a certificate or degree. The following are individual, selected courses designed to provide targeted education/exposure in specific AI subjects and topics, resulting at the conclusion in an enhanced level of AI literacy and proficiency. Many of the courses identified may also qualify for an educator's required annual continued professional development.

Teaching Tip

Quarter 1: Introduction to AI and Its Applications

Objective: Gain a foundational understanding of AI concepts, terminology, and its applications across various fields.
Suggested Courses:
AI For Everyone by Andrew Ng (Coursera)
Description: This course introduces the basics of AI, its capabilities, limitations, and potential uses in various industries. It's designed for those without a technical background.
Duration: 3 weeks, 2 hours per week
Mode: Virtual
URL: AI For Everyone (https://tinyurl.com/4myxezkz)
Elements of AI by the University of Helsinki
Description: A beginner-friendly course that covers the fundamentals of AI, including basic AI concepts and practical implications.
Duration: 6 weeks, self-paced
Mode: Virtual
URL: Elements of AI (www.elementsofai.com)
Activities:

- Discussion Groups: Join or form educator discussion groups to talk about the societal implications of AI.
- Literature Review: Read introductory AI books or articles focusing on AI in education.

Quarter 2: Understanding AI Tools and Basic Programming

- Objective: Get hands-on experience with AI tools and understand the basics of programming, especially as it relates to AI.
- Suggested Courses:
  - Introduction to AI with Python by Harvard University (edX)
    - Description: This course covers AI basics with a focus on Python programming, teaching how AI algorithms work.
    - Duration: 7 weeks, 10 hours per week
    - Mode: Virtual
    - URL: CS50 AI with Python (https://cs50.harvard.edu/ai/2024/)
    - Prerequisites: CS50x (introduction to the intellectual enterprises of computer science and the art of programming) or at least 1 year of experience with Python.
  - Introduction to TensorFlow for AI, ML, and DL (Coursera)
    - Description: A course on using TensorFlow for AI and machine learning, ideal for those who have some programming knowledge.
    - Duration: 4 weeks, 4 hours per week
    - Mode: Virtual
    - URL: TensorFlow on Coursera (www.coursera.org/learn/introduction-tensorflow)
    - Activities:
      - Project Work: Develop simple AI projects like a chatbot using available AI tools.
      - Peer Learning: Collaborate with other educators to build small AI-based teaching aids.

Quarter 3: AI in Education and Pedagogy

- Objective: Understand the integration of AI in educational settings and how it can enhance teaching and learning.
- Suggested Courses:
  - AI in Education by Microsoft
    - Description: Focuses on how AI tools can be used to support education, including personalized learning, administrative tasks, and student engagement.
    - Duration: 4 weeks, self-paced
    - Mode: Virtual
    - URL: AI in Education [https://learn.microsoft.com/en-us/training/educator-center/topics/ai-for-education]

AI Literacy for Educators (IBM Skills Network on Coursera)
  Description: A course aimed at educators, providing insights on how to teach AI concepts to students and incorporate AI into the curriculum.
  Duration: 4 weeks, 2–3 hours per week
  Mode: Virtual
  URL: AI Literacy for Educators (www.coursera.org/search?query=%20AI%20Literacy%20for%20Educators)
  Activities:

  - Lesson Planning: Create lesson plans that integrate AI tools, like AI-driven assessments or adaptive learning platforms.
  - Workshop Attendance: Attend virtual workshops or webinars on AI in education.

Quarter 4: Advanced AI Concepts and Capstone Project

Objective: Deepen understanding of advanced AI topics and complete a capstone project that demonstrates the application of AI in a teaching context.
Suggested Courses:
 Professional Machine Learning Engineer Certification (Google Cloud)
  Description: A more advanced course focusing on machine learning models and AI application development, suited for those with some technical background.
  Duration: 6 months, 4 hours per week
  Mode: Virtual
  URL: Google Cloud Certification (https://cloud.google.com/learn/certification/machine-learning-engineer)
 Capstone Project: Implementing AI in the Classroom
  Description: Design and implement a small-scale AI project in your classroom, such as an AI-powered teaching assistant, and document the process. Or create a year-long lesson plan (in detail that can be followed by your academic peers) that guides students from an entry-level understanding of AI to one of confident literacy.
  Duration: Entire quarter
  Mode: Virtual/In-Person (depending on the project)
  Activities:

  - Reflection: Write a reflective essay on your AI learning journey and how it has transformed your teaching practices.
  - Project Presentation: Present your capstone project to peers at one of the following educational technology conferences.
    1. International Conference on Artificial Intelligence in Education (AIED)

       Focus: The AIED conference is one of the leading forums for researchers and practitioners to present cutting-edge work in AI and its application to education.

2. URL: AIED Conference (www.aied2024.org)

   International Conference on Computers in Education (ICCE)

   Focus: ICCE covers a wide range of educational technologies, including AI, and welcomes contributions from K—12 educators, including middle school teachers.

   URL: ICCE Conference (https://conferenceindex.org/conferences/computer-education)
3. Society for Information Technology and Teacher Education (SITE) Conference

   Focus: The SITE Conference provides a platform for educators and researchers to share innovative applications of technology, including AI, in teaching and teacher education.

   URL: SITE Conference (https://site.aace.org)

This proposed AI literacy plan is flexible, allowing the educator to adapt the courses and activities based on their pace and interest. By the end of the year, the educator should have a solid foundation in AI, practical experience with AI tools, and a clear understanding of how to incorporate AI into their teaching practices.

As AI continues to deeply affect various aspects of education, educators must remain current with these technological advancements. Continuous professional development in AI assists educators in remaining competent and confident in using these tools, thus enhancing their approaches to teaching thus, ultimately improving student outcomes. By embracing AI literacy, educators are better equipped to prepare students for a future where technology plays an integral role in virtually every aspect of life, making AI proficiency a cornerstone of modern, global educational practice.

Using AI vs. Abusing AI

AI technology is double-sided. As discussed, there are many uses for AI, and these applications are growing daily. At the same time, with its widening implementation, and ease of use, there is a temptation to turn to AI for all one's needs, ultimately abusing AI.

Educators should address this fine line between use and abuse, fully prepared to discuss with students the benefits as well as the drawbacks of an overreliance on AI.

Table 1.6 provides a general comparison between an ethical non-abusive use of AI in education and an over-dependency or abuse of AI. Educators may wish to incorporate this information into a class exercise focusing on AI uses, limitations, and abuses. Tangentially, this provides an excellent opportunity to review and discuss the ethics of AI with your students.

Table 1.6 Using vs. Abusing AI

POSITIVE USES OF AI IN THE CLASSROOM	POTENTIAL ABUSES OF AI BY STUDENTS
Personalized Learning: AI can tailor educational content to fit each student's learning pace, strengths, and weaknesses, providing individualized support and resources.	**Cheating on Assignments**: Students might use AI tools like essay generators or problem-solvers to complete assignments without putting in the necessary effort, leading to academic dishonesty.
Automated Grading: AI can help educators by automating the grading process, providing quicker feedback and freeing up time for more student interaction.	**Plagiarism**: AI tools can generate essays or solve problems that students might present as their own work, leading to issues with plagiarism.
Enhanced Engagement: AI-powered educational games and simulations can make learning more interactive and engaging, especially for younger students.	**Manipulating AI Tutors**: Students might find ways to exploit AI-based tutoring systems to give them answers directly rather than learning the material.
Data-Driven Insights: AI can analyze student performance data to help teachers identify areas where students are struggling, allowing for timely intervention.	**Gaming the System**: Students might try to outsmart AI systems that track their progress by engaging in behaviors that improve their metrics without truly understanding the material.
Supporting Special Needs: AI tools can provide additional support for students with disabilities, such as speech-to-text for students with dyslexia or personalized learning paths for those with learning disabilities.	**Overreliance on AI**: Students may become too dependent on AI tools for answers and fail to develop critical thinking and problem-solving skills.
Adaptive Testing: AI can create adaptive tests that adjust in real time to a student's ability level, providing a more accurate assessment of their knowledge.	**Avoiding Challenging Content**: Students might use AI to skip difficult content by generating simplified summaries or answers, thus avoiding deeper learning.
Virtual Classrooms: AI can facilitate virtual learning environments, making education more accessible to students who cannot attend in person.	**Disengagement:** Overuse of AI for learning might lead to decreased engagement with teachers and peers, as students might prefer interacting with AI over humans.
Language Translation: AI can provide real-time language translation for students who are non-native speakers, making content more accessible.	**Automating In-Class Participation**: Students might use AI to generate responses during class discussions or online forums, leading to superficial participation.
Educational Content Creation: AI can assist teachers in creating content, such as quizzes and lesson plans that are tailored to the curriculum and student needs.	**Fabricating Data**: Students might use AI to fabricate data for assignments or projects, presenting false information as research findings.
Behavioral Insights: AI can analyze patterns in student behavior to identify those who might need additional support, whether academically or emotionally.	**Circumventing Learning Platforms**: Students might use AI tools to bypass or hack into learning platforms, gaining unauthorized access to tests or answers.

OpenAI. 2024. ChatGPT (August 24, 4o version) [Large language model]. Retrieved from [www.openai.com]. "Comparison of Positive Uses of AI in Education vs. Potential Abuses by Students." Table created by authors, August 24, 2024.

Summary

The focus of this chapter shifts from solely teaching good character to also teaching leadership development to seventh- and eighth-grade students. The chapter emphasizes that while character education remains important, students at this age should also be exposed to and learn about leadership qualities and how to apply them in both personal and digital contexts. Developing leadership skills alongside good character traits is essential for preparing students to be successful in both real-world and online environments.

This chapter highlights the impact of bullying both in the classroom and via social media. As leadership and ethical behavior become more ingrained in the student's daily life, making good choices against bullying behavior and the decision-making process. While encouraging independence, we also want to instill a sense of what is appropriate in various situations, so students do not succumb to peer pressure.

The role of AI in modern education, particularly in the context of leadership and character development for seventh- and eighth-grade students, is introduced in this chapter. AI is presented as a powerful tool that enhances learning by personalizing educational experiences and fostering creativity. Through the use of AI tools, students can receive customized learning and receive tailored feedback while developing essential digital literacy skills. The use of AI tools not only supports academic growth but also helps students build critical thinking and problem-solving abilities, preparing them for future challenges in an increasingly AI-centric, digitally infused-and dependent world.

The chapter also discusses the ethical implications of AI, emphasizing the importance of integrating character education with the responsible use of technology. Students are encouraged to apply leadership qualities like integrity and responsibility in their interactions with AI tools, ensuring that they use these technologies in ways that promote cyber safety and positive digital citizenship. By understanding and embracing AI while adhering to ethical standards, students can navigate the complexities of the digital age with confidence and become well-equipped leaders capable of making informed, ethical decisions in both online and offline environments.

LESSON PLANS

Grade 7

TOC Title: G7 Acceptable Behavior
Lesson Title: Acceptable Behavior
Grade Level: 7
Duration: 50 minutes

Objective:

- The students will understand acceptable behavior in different settings.
- The students will be able to identify the consequences of unacceptable behavior and the benefits of acceptable behavior.
- The students will know and be able to use strategies to make positive choices in social interactions.

Suggested Materials:

- Whiteboard and markers.
- Chart paper.
- Printed scenarios (provided below).

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask the class what the term acceptable behavior means to them.
b. Ask if they can think of sometimes when behavior might be acceptable in one place but not in another (e.g., classroom vs. playground).
c. Write students' answers on the board and guide them to think about acceptable behavior as being respectful and appropriate to the situation.

Acceptable/Unacceptable Behavior (15 minutes):

a. Explain that acceptable behavior is the way we act that shows respect for others and ourselves. It varies by setting (school, home, online, etc.).
b. Provide examples of acceptable behaviors in different contexts.
c. Examples:
    - School: Raising your hand before speaking, listening when others are talking.
    - Home: Helping with chores, speaking respectfully to family members.
    - Online: Not sharing personal information, being respectful in online comments.
    - Public Spaces: Waiting your turn in line, being quiet in a library.

d. Unacceptable Behavior: Discuss what happens when we engage in unacceptable behavior, such as hurting others' feelings, facing consequences like detention, or damaging relationships. Reinforce the idea that unacceptable behavior is anything that disrespects others, breaks the rules, or makes other people feel uncomfortable.

Group Activity (15 minutes):

a. Divide the class into small groups (three to four per group) and provide each group with a scenario. Each group will act out how to respond to the situation in a way that reflects acceptable behavior.
b. After each role-play, discuss as a class why the behavior and response were acceptable or unacceptable and how different choices could change the outcome.

Conclusion (10 minutes):

a. Ask students to reflect on their own behavior and think of one situation where they could have made a better choice.
b. Discuss the long-term benefits of practicing acceptable behavior, such as building trust, maintaining friendships, and creating a positive environment.

Assessment:

a. An informal assessment can be taken based on student participation in class discussions and activities.

Scenarios for Activity:

Scenario 1: A friend is being teased online.

Scenario 2: Someone cuts in front of you in line.

Scenario 3: You feel upset because a teacher corrected you in class.

Scenario 4: A friend wants to copy your homework.

Scenario 5: A student is spreading gossip and wants you to join in.

Scenario 6: Your friends want you to sneak off campus to go to a nearby store and buy candy.

Scenario 7: You are playing a game with friends, and one of them starts to cheat to win.

Scenario 8: You disagree with something your teacher said in class. You feel like they were unfair to you, and you are upset.

TOC Title: G7 Ethics & Leadership
Lesson Title: Ethics & Leadership
Grade Level: 7
Duration: 45 minutes

Objective:

- The students will understand the concept of ethics.
- The students will know the key traits of ethical leadership.
- The students will be able to apply ethical decision-making to real-world scenarios.

Suggested Materials:

- Whiteboard and markers
- Printed or written case studies for group work (included below)
- Paper and pencils/pens for individual reflection

Procedure

Introduction (10 minutes):

a. Whole group discussion: ask students what they think ethics means. Ask for examples of leaders they look up to, and why.
b. Write responses on the board, focusing on their understanding of right and wrong and traits of leaders they admire (e.g., honesty, responsibility).
c. Explain to students that ethics are the rules we follow in society about right and wrong.
d. Discuss leadership and how a good leader must be ethical in order to positively influence others.

Group Activity: Ethical Dilemmas (20 minutes)

a. Split students into small groups and give each group a case study with an ethical dilemma.
b. Ask each group to discuss the scenario and decide what an ethical leader would do in that situation. Write their answers on paper.
c. After 10 minutes, have each group present their case and solution. Encourage open discussion and emphasize ethical decision-making.

Individual Reflection (10 minutes)

Have students write on a piece of paper:

a. One thing they can do to be an ethical leader in their school or community.
b. A time when they made a difficult ethical decision and what guided them (how did they make their decision).

Conclusion (5 minutes):

- Summarize the importance of ethics, morals, and leadership.

Assessment:

a. An assessment can be taken based on participation in activities/discussions and on the individual reflection assignment.

Case Studies:

1. **Found Money**

   You are walking in the school hallway and find a $20 bill on the floor. You did not see anyone drop it, and no one seems to be around. What should you do?

2. **Group Project Conflict**

   You are working on a group project. One of your group members is not doing their part and the project is due tomorrow. The rest of the group is frustrated, and some members want to leave that person's name off the project. What is the right thing to do?

3. **Cheating on a Test**

   During a test, you notice a classmate copying answers from another student. The teacher does not notice, and your classmate asks you not to say anything. How do you handle this situation?

4. **Online Bullying**

   You see a classmate being bullied on social media. The person being bullied has not told anyone and seems very upset, but you are worried that if you tell an adult, the bullying might get worse. What would an ethical leader do in this situation?

5. **Favoritism in Sports**

   You are part of the school's soccer team. The coach always picks their favorite players for important positions, even though some other students are more skilled. You are one of the better players, but you notice the unfairness. Should you speak up, stay quiet, or talk to the coach privately?

6. **Lying to Avoid Trouble**

   You accidentally broke a window in the classroom while playing, but no one saw you do it. Later, a teacher asks the class who was responsible. Some students blame someone else. Should you admit to what happened, or let the other student take the blame?

7. **Excluding a Friend**

   Your group of friends decides not to invite a particular student to a school event because they think that person is “weird”. You feel bad about excluding someone, but you do not want to upset your friends. What should you do?

8. **Plagiarism on a Report**

   You are assigned a big report, and you find a perfect paper online that covers exactly what you need. You are running out of time to finish, and it would be easy to copy and submit it. No one would know, but it would not be your work. What should you do?

9. **Peer Pressure to Skip Class**

   Some classmates want to skip class to hang out. They ask you to come along and say no one will notice if you are all gone. You do not want to miss class, but you also do not want to seem “uncool” by saying no. How should you handle the situation?

10. **Taking Credit for Someone Else’s Work**

    In an art class, a student left their project unattended, and you accidentally get praised for their work. The teacher and other students think it is yours, and you are not sure if you should correct them. How would a responsible leader act?

TOC Title: G7 Cyberbullying
Lesson Title: Cyberbullying
Grade Level: 7
Duration: 50 minutes

Objective:

- Students will understand the impact of cyberbullying.
- Students will be able to recognize its different forms.
- Students will know and be able to use strategies for prevention and response to cyberbullying.

Suggested Materials:

- Internet access for video (optional).
- *Let's Fight It Together* (6 minutes 30 seconds). https://www.youtube.com/watch?v=dubA2vhIlrg, or a similar age-appropriate video.
- Printed copies of scenarios for role-play activity (provided below).
- Writing materials.

Procedure

Introduction (10 minutes):

a. Begin with a brief discussion of what cyberbullying is. Ask students if they have heard of "cyberbullying"? What does it mean? Why do they think cyberbullying happens online rather than in person?
b. Define cyberbullying as any type of bullying that occurs online. Include examples like spreading rumors, sending harmful messages, or sharing embarrassing photos.

Video and discussion (15 minutes):

a. If showing the video "Let's Fight It Together" by Childnet International, or a similar age-appropriate video.
b. After the video, discuss the following:
    - What happened in the video?
    - How did the victim feel?
    - How do you think you would feel in that situation?
    - What could have been done differently to prevent or stop the cyberbullying?

Group Activity: Role-Playing Scenarios (15 minutes):

a. Divide students into small groups and give each group a different cyberbullying scenario.
b. Each group will develop a short role-play that shows both the cyberbullying incident and a positive way to resolve it.

Conclusion (10 minutes):

a. Have students write a short reflection on what they learned about cyberbullying and how they can be part of the solution.
b. Encourage students to share their thoughts with the class.

Assessment:

a. Participation in group activities and discussions.
b. Written reflection on the lesson's content.

Role-Play Scenarios:

1. Mean Comments on a Post
    - Scenario: A student posts a picture of their new haircut on social media. Another student leaves a series of mean comments, making fun of their appearance. Soon, others join in, sharing rude remarks.
    - Role-Play Focus: How the victim feels, what friends or bystanders could do, and how to report harmful comments.
2. Exclusion from a Group Chat
    - Scenario: A group of friends creates a new group chat, but purposely leaves one student out, sharing jokes and plans without them. When the excluded student asks why they weren't added, they are met with silence or are teased for being "annoying."
    - Role-Play Focus: Feelings of exclusion, how exclusion is a form of bullying, and how to include others fairly.
3. Spreading a Meme
    - Scenario: Someone takes a picture of a student in a funny pose and turns it into a meme, spreading it around the school without permission. Soon, the meme goes viral, and students start making fun of the person involved.
    - Role-Play Focus: Discussing permission when sharing images, the long-term impact of viral posts, and how the situation can be resolved.
4. Pretending to Be Someone Else (Impersonation)
    - Scenario: A student creates a fake social media account pretending to be someone else from school. They start posting embarrassing or hurtful things, making it seem like the victim is saying those things.
    - Role-Play Focus: The emotional impact of impersonation, how it damages someone's reputation, and how to report fake accounts to platform administrators.
5. Secretly Recording and Sharing
    - Scenario: During a Zoom call for school, one student secretly records another student doing something embarrassing (like falling off their chair) and then shares the clip with the entire class.
    - Role-Play Focus: Privacy issues, the embarrassment caused by unwanted sharing, and how to handle peer pressure to share inappropriate content.
6. Rumors Spread Online
    - Scenario: A student starts a false rumor on social media that another student cheated on an important test. The rumor spreads quickly, leading to negative comments and people avoiding the accused student.
    - Role-Play Focus: The harmful effects of spreading false information, how rumors can damage reputations, and how to confront or stop the rumor.

7. Hurtful Messaging in a Game Chat
    - Scenario: While playing an online multiplayer game, a group of students starts sending mean messages to one player for not playing well. They gang up, calling the player names and telling them to leave the game.
    - Role-Play Focus: Online etiquette in gaming, how to deal with bullying in gaming spaces, and when to report players for abusive behavior.
8. Mocking Someone's Post
    - Scenario: A student shares a personal post about something important to them (e.g., family tradition, favorite hobby), but classmates mock the post with rude emojis, GIFs, or sarcastic comments.
    - Role-Play Focus: How mocking someone's interests or values online can hurt, how to support the victim, and ways to deal with sarcasm and online disrespect.
9. Fake Poll
    - Scenario: A student creates an online poll titled "Who is the most annoying person in our class?" and shares it with everyone. Classmates start voting, and the student with the most votes finds out and feels devastated.
    - Role-Play Focus: The power of online voting, how anonymous polls can lead to bullying, and the responsibility of others to shut it down.
10. Exposing a Secret
    - Scenario: A student tells their friend a personal secret via text, but the friend screenshots the message and shares it with others. Soon, the secret is all over school.
    - Role-Play Focus: Trust in friendships, why sharing private information can cause harm, and how to handle situations when trust is broken.

TOC Title: G7 Disability Bullying
Lesson Title: Disability Bullying
Grade Level: 7
Duration: 40 minutes

Objective:

- The students will understand what disability bullying is and how it affects individuals.
- The students will gain understanding of and empathy toward people with disabilities.
- The students will know and use strategies to support peers with disabilities.

Suggested Materials:

- Whiteboard or Smartboard.
- Markers.
- Journals or paper for reflective writing. There are several online journals such as Grades 7 and 8 Prompts » JournalBuddies.com, which may be helpful.

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask students for a definition of bullying. Write their answers on the board.
b. Ask what they think bullying someone with a disability looks like.
c. Allow students to discuss and provide examples.
d. Explain that disabilities can be physical, intellectual, sensory, or mental, and that bullying people with disabilities is harmful because it targets a part of who they are.
e. Highlight the importance of respect and inclusion.

Group Discussion (10 minutes):

a. Ask the class the following questions and write key points made by students on the board.
    - What are some misconceptions that people have about students with disabilities?
    - How does bullying impact someone emotionally and socially, especially if they already face challenges because of a disability?
    - How can we stand up to bullying when we see it?

Interactive Empathy-Building Activity (15 minutes):

a. Break students into small groups. Assign each group a "disability challenge." (If resources are limited, you can choose one activity for the whole class.)
    - Vision impairment: Students wear blindfolds and try to navigate a short path or write their name on a piece of paper.
    - Hearing impairment: Some students cover their ears, and the other students speak to them. Then, ask how well they could hear and how it made them feel.
    - Mobility impairment: Students try to do simple tasks like picking something up or moving around while keeping one leg immobile (e.g., hopping on one leg).

b. After 10 minutes of activities, come back together and ask:
    - How did it feel trying to complete the task?
    - How would bullying someone with this challenge affect them even more?

Conclusion (5 minutes):

a. Ask students to reflect on what they learned.
b. Challenge them to think of one way they can be more inclusive and supportive of students with disabilities.
c. Conclude with the idea that everyone has differences, but bullying someone because of those differences is never okay. It's important to stand up, speak out, and be an ally.

Assessment:

a. An informal assessment can be made based on student participation in activities and discussions.

TOC Title: G7 Emotional Bullying
Lesson Title: Emotional Bullying
Grade Level: 7
Duration: 35 minutes (43 minutes with suggested video)

Objective:

- The students will be able to define emotional bullying.
- The students will recognize the signs of emotional bullying.
- The students will know and be able to use strategies to stop bullying and support others.
- Optional anti-bullying video. Suggestion: *Anti-Bullying (short film)*, https://www.youtube.com/watch?v=DA6wjqAY9O4 (7 minutes 47 seconds), or a similar age-appropriate video.

Suggested Materials:

- Whiteboard and markers.
- Sticky notes.
- Pens/pencils.

Procedure

Introduction (10 minutes):

a. Ask students to write down one word that comes to mind when they think of "bullying" on a sticky note and place it on the board.
b. Group the sticky notes into categories (e.g., physical, verbal, emotional). Highlight the "emotional" category, explaining that today's focus is on emotional bullying.
c. Define emotional bullying as causing emotional hurt to another person. This can include saying or writing hurtful things, causing others to gang up on an individual, and purposely ignoring, or spreading rumors.

Empathy and Impact (10 minutes 18 minutes with suggested video):

a. Show anti-bullying video. Suggestion: *Anti-Bullying (short film)*, https://www.youtube.com/watch?v=DA6wjqAY9O4, or a similar age-appropriate video.
b. Ask students to imagine how they would feel if they were the target of emotional bullying. Have them write down those feelings on a piece of paper.
c. If possible, have the class sit in a circle. Ask volunteers to share how they would feel. Emphasize the importance of empathy and understanding how deeply emotional bullying can affect someone.

Creating a Supportive Environment (10 minutes):

a. Brainstorm Solutions: On the whiteboard, list ways to stop emotional bullying and support those affected (e.g., speaking up, being kind, including others, reporting to an adult).
b. Pledge: Have students create a class pledge against emotional bullying, including actions they can take to foster a positive and inclusive environment.

Closing Reflection (5 minutes):

a. Reflection: Ask students to write down one action they will take to prevent emotional bullying on a positive affirmation card.

Assessment:

a. An informal assessment can be made based on participation in activities and discussions.

TOC Title: G7 Personal Bullying
Lesson Title: Personal Bullying
Grade Level: 7
Duration: 40 minutes

Objective:

- The students will be able to define personal bullying.
- The students will know and be able to use strategies to prevent and respond to personal bullying in ways that promote self-empowerment and a positive school environment.

Suggested Materials:

- Whiteboard/Markers or Smartboard
- Handouts on bullying definition, types, and resources (Table LP 1.7)
- Scenario cards for group activity (Scenarios below).

Procedure

Introduction (5 minutes):

a. Ask students what the word *bullying* means.
b. Encourage various responses and write key responses on the board.
c. Clarify that personal bullying refers to any type of bullying that is related to a person's gender or sexuality.

Discussion: (10 minutes):

Discussion Questions:

a. Ask the class the following questions and allow volunteers to share responses.
    - How do you think bullying based on gender or sexuality impacts the person being bullied?
    - How does this affect others who witness the bullying?

Empowerment Strategies (5 minutes):
Share the following strategies with the class. Write them on the board or chart paper for reference during the scenario activity.

a. Speaking Up: Encourage students to use their voices to say, "That's not okay," when they witness personal bullying.
b. Supporting Peers: Suggest ways they can support classmates who are being bullied by checking in on them, inviting them to join activities, or showing them they are not alone.

c. Reporting: Reinforce the importance of telling a teacher, counselor, or trusted adult when they see bullying happening.
d. Respectful Language: Teach students the importance of using inclusive language. Avoiding hurtful jokes or slurs, and being mindful of how words impact others.

Group Activity: Problem-Solving Scenarios (15 minutes):

a. Divide students into small groups and give each group a scenario card that describes a personal bullying situation (e.g., a student being teased for having two dads, or being bullied for not conforming to gender norms).
b. Each group discusses how they would handle the situation in a way that empowers both the person being bullied and the bystanders. Focus on respectful and proactive solutions.
c. Encourage students to think of actions like speaking up, supporting the person being bullied, or reporting it to an adult.

Conclusion (5 minutes):

Summarize Key Points:

a. Personal bullying is hurtful and unacceptable.
b. We all have the power to create a supportive and kind environment.
c. It is important to stand up for others and promote respect for everyone regardless of how they identify.

Assessment:

a. Take an informal assessment based on participation in discussions and group activity (Table LP 1.7).

Table LP 1.7 Nine Bullying Types

BULLYING TYPE	DEFINITION	POSSIBLE USE
Cyberbullying	Any type of bullying that happens online. It can be hurtful comments on a personal site or deceptive private messaging.	Email, cell phones, text messages, and Internet sites to threaten, harass, embarrass, socially exclude, or damage reputations and friendships.
Disability bullying	Leaving someone out or treating them badly because of a disability.	Making someone feel uncomfortable or making jokes to hurt someone because of a disability. On a physical level, it includes harmful actions such as blocking ramps and elevators, tripping, or tampering with accessible equipment. Online disability bullying may include making jokes to make the individual feel uncomfortable or "less than" and circulating memes of disabled people in a way that makes fun of the individual's disability.
Emotional bullying	Using ways to cause emotional hurt (nonphysical and unseen) to another person.	Saying or writing hurtful things, causing others to gang up on an individual, and purposely ignoring, or spreading rumors. Online emotional bullying may include addressing comments directly to the person via social media sites or chat rooms with the intent to embarrass the person.
Personal bullying	Any sort of bullying, done in any manner that is related to a person's gender or sexuality, to make them feel uncomfortable because of their sexuality.	Making sexist comments or jokes; touching, pinching, or grabbing someone in a sexual way; making crude comments about someone's sexual behavior or orientation; or spreading a sexual rumor. Online personal bullying may include direct comments regarding the victim's appearance, hair, clothing, or general style. This may include hacking the person's account to appear as the account owner.
Physical bullying	Always involves some type of physical contact with the other person.	Hand-to-hand, but it can also mean throwing items, tripping, or eliciting others to cause physical harm to a person. This type of bullying can also cause harm to property and belongings.
Racial bullying	Treating people badly because of their racial or ethnic background.	Saying bad things about a cultural background, calling someone racist names, or telling racist jokes. Online racial bullying may include "flaming" where language and insults are used to insult or intimidate the target.
Religious bullying	Treating people badly because of their religious background or beliefs.	Making negative comments about a religious background or belief, calling someone names, or telling jokes based on his or her religious beliefs to hurt them. Online religious bullying may include making jokes about their belief to make them feel uncomfortable and posting demeaning memes of religious dress, food, or leaders.
Social bullying	Excluding others from the group, getting others to ignore or exclude.	Ranges from rolling your eyes or turning away from someone, gossiping or spreading rumors, setting others up to look foolish, to damaging reputations and friendships. Online social bullying may include creating fake events like a party and posting pictures of friends to make the victim feel excluded from the event, or fake accounts in someone the victim's name to post negative or inappropriate comments or images.
Verbal bullying	Using any terms or actions that cause the other person distress. Examples include	Using profanities, hurtful language, negatively commenting on a person's appearance, using derogatory terms, or teasing. Online verbal bullying may implement this type of language and include a call to action for others to join the verbal abuse against the person being bullied.

Scenarios for Group Activity on Personal Bullying:

1. Scenario 1: “That’s for Boys!”
   A student in your class loves sports and is always excited to play soccer during gym class. One day, some classmates start teasing them, saying, “Soccer is for boys, not girls!” The student looks upset and doesn’t want to play anymore.

2. Scenario 2: “Stop Acting So Girly”
   During lunch, a student talks about their favorite TV show, which is known for being popular with girls. A group of students overhears and starts mocking him, saying, “Stop acting so girly!” The student becomes quiet and looks embarrassed.

3. Scenario 3: “You Can’t Have Two Dads!”
   A student mentions that they have two dads when talking about their family. Some classmates react by laughing and saying, “That’s so weird! You can’t have two dads!” The student looks hurt and doesn’t talk for the rest of the conversation.

4. Scenario 4: “Why Do You Dress Like That?”
   One student prefers wearing clothes that are different from what other girls usually wear. One day, a group of students points and says, “Why do you dress like that? You should wear normal girl clothes.” The student seems embarrassed and tries to ignore them.

5. Scenario 5: “Are You Gay?”
   A student becomes close friends with someone of the same gender, and some classmates begin teasing them, saying, “Are you two dating? You must be gay!” The student feels uncomfortable and doesn’t know how to respond.

6. Scenario 6: “That’s Not Normal”
   During a group project, a student shares that their sibling is nonbinary (someone who doesn’t identify as strictly male or female). Another student says, “That’s not normal. Why can’t they just pick?” The student sharing feels uncomfortable and doesn’t say anything else.

7. Scenario 7: “Boys Don’t Cry”

   After receiving a bad grade on a test, a student starts tearing up. Another student says, “Boys don’t cry. Are you a girl or something?” The student wipes their tears and stays quiet for the rest of the class.

8. Scenario 8: “You’re Too Girly to Play with Us”

   A student who identifies as a girl wants to join a game of basketball during recess. The other kids, mostly boys, say, “You’re too girly to play with us,” and walk away, leaving the student feeling left out.

TOC Title: G7 Physical Bullying

Lesson Title: Physical Bullying
Grade Level: 7
Duration: 45 minutes

Objective:

- The students will be able to identify physical bullying.
- The students will understand the impact of physical bullying.
- The students will be able to show empathy toward victims of bullying.

Suggested Materials:

- Whiteboard
- Journals or notebooks. There are several online sites and free resources for journaling. Here is one specifically for teens that may provide journaling ideas. Grades 7 & 8 Prompts » JournalBuddies.com.
- Short video clip on physical bullying. Suggestion: *I Survived Extreme Bullying – Suede Brooks – storybooth Star*s, https://www.youtube.com/watch?v=xss9zDfINXI (3 minutes 34 seconds), or a similar age-appropriate video.
- Copies of an empathy-building scenario (optional).

Procedure

Introduction (10 minutes):

a. Begin by asking students what they think physical bullying is. Write key terms on the board such as hitting, pushing, intimidation, and violence.
b. Discuss the physical and emotional impact of physical bullying. Highlight how it can leave lasting scars, both visible and invisible.

Video Clip (10 minutes):

a. Show the suggested video or another age-appropriate video that depicts a scenario of physical bullying.
b. Ensure it focuses on the victim's experience and the emotions involved.
c. After the video, ask students the following:
    - How did the bullying make the victim feel?
    - What could have been done differently by bystanders or the bully?

Activity (15 minutes):

a. Ask students to journal their thoughts on one of the following prompts (write prompts on the whiteboard):

- Prompt 1: "Describe a time when you witnessed or experienced physical bullying. How did it make you feel, and what do you wish had been done?"
- Prompt 2: "If you were a bystander to physical bullying, what would you do to help? Why?"
- Prompt 3: "If you were the bully, how would you feel if someone physically bullied you? What do you think you would do differently?"
- Encourage students to focus on the emotional and personal side of the experience to build empathy.

Conclusion (10 minutes):

a. After journaling, invite volunteers to share their entries (optional).
b. Lead a reflective discussion: How did writing about the situation change their perspective? What emotions came up while writing?

Assessment:

a. Participation in group activities and discussions.
b. Optional: Review journals focusing on thoughtfulness and effort (not for grammar/spelling so as not to diminish creative journaling style).

TOC Title: G7 Racial Bullying

Lesson Title: Racial Bullying

Grade Level: 7

Duration: 55 minutes (58 minutes with video). Consider splitting this lesson plan into two sessions based on time allocated.

Objective:

- The students will be able to define and recognize racial bullying.
- The students will understand the harmful effects of racial bullying on individuals and communities.
- The students will know and be able to use strategies to prevent and respond to racial bullying.

Suggested Materials:

- Whiteboard and markers.
- Projector (optional for videos — see suggested video below — or slides).
- Scenarios of racial bullying (provided below).
- Chart paper and markers (for group activity).

Procedure

Introduction (10 minutes):

a. Show a video about racial bullying – suggested video: Teenager subjected to racist cyberbullying wants parents, schools to fight hate (youtube.com) (2 minutes 30 seconds), or another age-appropriate racial bullying video.
b. Whole Group: Lead a brief discussion on what bullying is and the different types of bullying students are aware of.
c. Define Racial Bullying: Bullying based on someone's race, skin color, ethnicity, or culture. This includes name-calling, exclusion, stereotypes, or physical harm, and this can happen in person and online.

Class Discussion: The Impact of Racial Bullying (15 minutes):

a. Explain that racial bullying can lead to feelings of sadness, anger, and isolation. It can damage self-esteem and even lead to physical harm.
b. Ask "What are some examples of racial bullying that we've seen or heard about in the world?" (Encourage students to think about real-world examples from the news or media.)
c. Discuss how racial bullying affects not just the person being bullied but the entire community, as it creates divisions and fosters hate.

Group Activity: Identifying Solutions (15 minutes):

a. Divide students into small groups. Give each group a scenario of racial bullying.
b. Ask groups to come up with ways to address the situation.
c. Questions for Discussion in Groups:

  - What should the person being bullied do?
  - What can bystanders do to help?
  - How should a teacher or adult respond?

d. Chart Responses: Each group should write their ideas on chart paper.

Presenting Solutions and Class Discussion (10 minutes):

a. Have each group present their scenario and solutions.
b. After each group presents, ask the class if they agree with the solutions or if they can think of other ideas.
c. Emphasize the importance of being an upstander (someone who stands up to bullying and supports the victim) instead of a bystander.

Conclusion (5 minutes):

a. Summarize the lesson by asking students to share one thing they learned about racial bullying.

Assessment:

a. An informal assessment can be taken based on participation in discussions and activities.

Scenarios for Activity:

Scenario 1: The Lunchroom Incident

A student is sitting alone at lunch. A group of students walks by and makes comments about the student's food, saying things like "That smells gross. No wonder people from your country eat weird stuff." They laugh and move on, but the student looks upset and starts throwing their lunch away.

Discussion Questions:

1. How do you think the student feels?
2. What could someone do to help?
3. How could the students who made the comments change their behavior?

Scenario 2: The Group Project:

During a group project, one student makes a joke about another student's accent, saying, "How are we supposed to understand anything you say?" The group laughs, but the student with the accent looks embarrassed and doesn't speak much for the rest of the class.

Discussion Questions:

1. How might the student feel after the comment was made?
2. What should the group members do?
3. What is the role of the teacher or an adult in this situation?

Scenario 3: The Bus Ride

On the bus ride home, a group of students is teasing another student for wearing traditional cultural clothing. They make fun of how "different" it looks and ask, "Why don't you wear normal clothes like everyone else?"

Discussion Questions:

1. How do you think the student being teased feels?
2. What could a bystander on the bus do to help?
3. What should happen next to stop this from continuing?

Scenario 4: The Social Media Post

A student posts a picture on social media with a caption making fun of someone's race, using stereotypes and emojis that are offensive. Other students start commenting and adding their own jokes. The student being targeted sees the post and feels hurt.

Discussion Questions:

1. How could the student being targeted feel?
2. What can you do if you see this kind of post online?
3. What can teachers or adults do in this situation?

Scenario 5: The Physical Education (PE) Class

In PE class, a student is picked last for a team because other students say, "People from your country aren't good at sports." The student looks upset but doesn't say anything.

Discussion Questions:

1. How does it feel to be excluded based on a stereotype?
2. What could the other students do differently?
3. How can the teacher or coach help address this issue?

Scenario 6: The Name-Calling

A student walks into class, and another student makes a racial joke, calling them a name based on their skin color. Some of the classmates laugh, but others look uncomfortable. The student who was called the name looks hurt but tries to ignore it.

Discussion Questions:

1. How do you think the student who was called names feels?
2. What can the students who laughed or stayed silent do next time?
3. How could the teacher or school prevent this from happening?

Scenario 7: The Classroom Joke

During a history lesson, the teacher discusses different cultures around the world. One student makes a joke about a specific group, saying, “People from there are always lazy.” Some students laugh, but others look uncomfortable. The student from that culture doesn’t say anything, but their expression shows that they are hurt.

Discussion Questions:

1. How do you think the student from that culture feels hearing the joke?
2. What could the classmates do to stop this behavior?
3. What should the teacher do to address the situation in the moment?

Scenario 8: The Birthday Party Exclusion

A group of students is talking about an upcoming birthday party, inviting almost everyone in the class. One student overhears them saying that they aren’t invited because their family “does things differently” and they don’t want the student’s “weird” traditions at the party. The student feels excluded and ashamed.

Discussion Questions:

1. How would it feel to be excluded from a party based on cultural or racial differences?
2. What could the students do to be more inclusive?
3. What could a friend or bystander say to support the student who was excluded?

TOC Title: G7 Religious Bullying
Lesson Title: Religious Bullying
Grade Level: 7
Duration: 45 minutes (47 minutes with video)

Objective:

- Students will be able to define religious bullying.
- Students will understand the impact of religious bullying.
- Students will know and be able to use strategies to prevent religious bullying.

Suggested Materials:

- Chart paper and markers.
- Printed handouts with scenarios (scenarios below).
- Index cards.
- Pens or pencils.

Procedure

Introduction (10 minutes):

a. Show a short, age-appropriate video that depicts a scenario of physical bullying. Suggestion: *Religious Harassment & Bullying | #LikeThatThenHow | Being Community (youtube.com)* (1 minute 17 seconds), or a similar age-appropriate video.
b. Whole group: Review with the students what bullying is.
c. Define Bullying as the repeated hurting, threatening, or intimidating of a person by another person or group.
d. Introduce Religious Bullying: Explain that religious bullying is treating people badly because of their religious background or beliefs. Examples include making negative comments about a religious background or belief, calling someone names, or telling jokes based on his or her religious beliefs to hurt them.

Group Activity (20 minutes): Understanding Religious Bullying:

a. Divide students into small groups (three to four students): Give each group a piece of chart paper and markers.
b. Provide each group with different scenarios that depict instances of religious bullying.
c. Group Task: Each group discusses their scenario and writes down the following:
    - What is happening in the scenario?
    - How might the person who is bullied feel?
    - What could bystanders do to help?
d. Share and Discuss: Each group presents their scenario and findings. Discuss as a class.

Informal Assessment (10 minutes):

a. Distribute index cards and ask students to write down their responses to the following question: “What would you do if you saw someone being bullied because of their religion?”
b. Collect the Cards: Collect and review the cards to gauge students’ understanding and empathy. Provide feedback if necessary.

Conclusion (5 minutes):

a. Summarize the key points of the lesson.
b. Emphasize that everyone has a right to feel safe and accepted. Religious beliefs should not be a factor.

Assessment:

a. Review collected assessment cards for understanding.

Scenarios for Group Activity:

Scenario 1

Situation: Maria wears a headscarf to school as part of her religious practice. Some classmates call her names and pull at her scarf during recess.

Discussion Points:

1. What is happening in this scenario?
2. How might Maria feel?
3. What could the bystanders do to help?

Scenario 2

Situation: Ahmed cannot eat certain foods due to his religious dietary restrictions. During lunchtime, some students tease him for bringing different food from home and making jokes about his religion.

Discussion Points:

1. What is happening in this scenario?
2. How might Ahmed feel?
3. What could the bystanders do to help?

Scenario 3

Situation: Rachel celebrates different holidays than most of her classmates. When she talks about her holiday traditions, some students laugh and tell her that her holidays are weird.

Discussion Points:

1. What is happening in this scenario?
2. How might Rachel feel?
3. What could the bystanders do to help?

Scenario 4

Situation: John's religion requires him to pray before meals. At lunchtime, some students mock him by imitating his prayer gestures and making fun of him.

Discussion Points:

1. What is happening in this scenario?
2. How might John feel?
3. What could the bystanders do to help?

Scenario 5

Situation: Leah wears a necklace with a religious symbol. A group of students snatch it from her and say that her religion is stupid.

Discussion Points:

1. What is happening in this scenario?
2. How might Leah feel?
3. What could the bystanders do to help?

Scenario 6

Situation: During a class project, Sam mentions a story from his religious texts. His classmates roll their eyes and say they don't want to hear about his religion.

1. What is happening in this scenario?
2. How might Sam feel?
3. What could the bystanders do to help?

Scenario 7

Situation: Anika fasts during a religious observance. Some students make fun of her for not eating lunch and say she's just trying to get attention.

Discussion Points:

1. What is happening in this scenario?
2. How might Anika feel?
3. What could the bystanders do to help?

Scenario 8

Situation: David wears a small cap for religious reasons. A group of students continuously tease him, calling him "weird" and "different."

Discussion Points:

1. What is happening in this scenario?
2. How might David feel?
3. What could the bystanders do to help?

Scenario 9

Situation: Sarah is Hindu and wears a bindi on her forehead. Some students ask her if she's trying to look like a clown and make fun of her during class.

Discussion Points:

1. What is happening in this scenario?
2. How might Sarah feel?
3. What could the bystanders do to help?

Scenario 10

Situation: Emily is excluded from a group project because her classmates say they don't want to work with someone who has "weird religious beliefs."

Discussion Points:

1. What is happening in this scenario?
2. How might Emily feel?
3. What could the bystanders do to help?

TOC Title: G7 Social Bullying

Lesson Title: Social Bullying
Grade Level: 7
Duration: 40 minutes

Objective:

- The students will understand what social bullying is and the impact it has on others.
- The students will know and be able to use strategies to prevent or stop social bullying.

Suggested Materials:

- Whiteboard and markers.
- Handouts with scenarios of social bullying (provided below).
- Sticky notes and pens.
- Anti-bullying video. Suggestion: *Choices (Anti-Bullying Short Film)* (4 minutes 40 seconds), https://www.youtube.com/watch?v=kkom2BJOT1U), or a similar age-appropriate video.

Procedure

Introduction (10 minutes):

a. Class discussion: Ask students what they think bullying looks like.
b. Write their responses on the board.
c. Introduce social bullying as a form of bullying that involves hurting someone's reputation or relationships. It includes excluding others from the group and spreading gossip, and rumors. Online social bullying may include creating fake accounts to target the victim via abusive posts, and posts that are intended to make the victim feel excluded from social events.

Video and Activity (15 minutes):

a. Show an anti-bullying video. Suggestion: *Choices (Anti-Bullying Short Film)* (4 minutes 40 seconds), https://www.youtube.com/watch?v=kkom2BJOT1U, or a similar age-appropriate video.
b. Have students write down something they learned from the video and something they now feel can do about bullying.
c. Ask volunteers to share their thoughts with the class.

Strategies to Stop Social Bullying (15 minutes):

a. Write the following categories on the board:
  - For the Person Being Bullied
  - For the Bystanders
  - For the Bully.

b. Brainstorm with the class strategies for each category. Guide the class toward practical solutions such as follows:
  - **For the person being bullied:** Encourage them to talk to a trusted adult, build positive friendships, and remind them that it's not their fault.
  - **For the bystanders:** Teach them to speak up, support the victim, refuse to spread rumors, and report bullying to an adult.
  - **For the bully:** Encourage them to think about how their actions hurt others and how they can make things right.

Conclusion (5 minutes):

a. Have students write on a sticky note:
  - One thing they learned today.
  - One thing they will do differently moving forward.
  - Collect the sticky notes and discuss a few before ending.

Assessment:

a. Take an informal assessment of student participation in discussions and activities.

TOC Title: G7 Verbal Bullying
Lesson Title: Verbal Bullying
Grade Level: 7
Duration: 45 minutes

Objective:

- Students will understand what verbal bullying is and its impact.
- Students will identify ways to prevent and respond to verbal bullying.
- Students will feel empowered to create a supportive and respectful classroom environment.

Suggested Materials:

- Whiteboard and markers.
- Scenario cards (included below).
- Index cards and pens.

Procedure

Introduction (10 minutes):

a. Group discussion. Ask students what bullying is. Write down students' responses on the board. Guide the discussion toward types of verbal bullying, such as teasing, name-calling, and spreading rumors.
b. Define Verbal Bullying as using words to harm, threaten, or manipulate someone. It may include name-calling, insults, teasing, intimidation, or hurtful comments.
c. Discuss the impact of verbal bullying on both the victim and the school environment.

Activity (15 minutes):

a. Divide the class into small groups and give each group a scenario card describing a verbal bullying situation (e.g., teasing about appearance, spreading rumors, name-calling).
b. Ask groups to discuss and role-play how they might respond to the situation as bystanders or victims in a constructive way.
c. After the role-play, bring the class together to discuss what strategies worked best and how they felt during the exercise.
d. Discuss how standing up to verbal bullying can be empowering and beneficial for everyone.

Empowerment Strategies (15 minutes)

Developing a Response:

a. Introduce strategies for responding to verbal bullying, such as follows:
  - **Ignore**: Walk away and don't engage.
  - **Respond assertively**: Use "I" statements (e.g., "I don't like it when you talk to me that way").
  - **Seek help**: Talk to a trusted adult or peer.
  - **Support others**: Be an ally to those who are bullied by standing up for them or offering support.

Conclusion (5 minutes):

Reflective Writing:

a. Provide each student with an index card. Ask them to write down one action they will take to prevent verbal bullying in their school.
b. Collect the cards and share some responses anonymously to reinforce the collective commitment.
c. Summarize the lesson by highlighting key points about recognizing and preventing verbal bullying.
d. Encourage students to share any final thoughts or questions.

Assessment:

a. Observe student participation in discussions and role-plays.
b. Review the reflective index cards to assess students' understanding and commitment to preventing verbal bullying.

Scenarios for Role-Playing Activity:

Scenario 1: Name-Calling in Class

One of your classmates, Alex, often calls you mean names in front of others during class. This happens regularly, and sometimes other students laugh. It makes you feel embarrassed and upset.

Discussion Questions:

1. How do you think Alex's words make the victim feel?
2. What can you do if you're the victim?
3. How can a bystander help in this situation?

Scenario 2: Spreading Rumors

Jordan starts spreading a rumor about another student, Casey, saying that Casey cheated on a test. The rumor isn't true, but it starts spreading quickly, and people are making fun of Casey.

Discussion Questions:

1. How might spreading rumors affect Casey?
2. What could you do if you hear someone spreading rumors?
3. How can you support Casey?

Scenario 3: Teasing about Appearance

Samantha gets teased every day at lunch about her hairstyle and clothes. A group of students keeps making fun of her, saying things like "Nice clothes from last century!" Samantha usually tries to ignore it, but it's starting to get to her.

Discussion Questions:

1. How can Samantha respond to the teasing?
2. What would you do if you were a friend of Samantha?
3. How can teasing about someone's appearance impact them?

Scenario 4: Insulting Someone's Interests

Ryan is really into reading comic books, but another student, Taylor, keeps saying, "Comics are for babies!" and "Why don't you grow up?" Taylor's comments make Ryan feel bad about his interests.

Discussion Questions:

1. Why might it be hurtful to insult someone's hobbies?
2. What should Ryan do to handle Taylor's comments?
3. How can a bystander step in to support Ryan?

Scenario 5: Making Fun of Someone's Mistake

During a group presentation, Lily accidentally reads a word wrong, and a student, Mia, loudly mocks her mistake, saying, "Wow, are you in first grade or something?" This makes Lily feel embarrassed in front of the class.

Discussion Questions:

1. What impact might Mia's comment have on Lily?
2. How can Lily respond to Mia's remark?
3. What could the teacher or other students do to address the situation?

Scenario 6: Exclusion from a Group

Ethan wants to join a group project with some classmates, but one of the group members, Sean, says, "We don't want you on our team; you're not good enough." Ethan feels excluded and hurt.

Discussion Questions:

1. How does exclusion act as a form of verbal bullying?
2. What could Ethan do in this situation?
3. How can the group change their behavior to be more inclusive?

Scenario 7: Sarcasm and "Joking"

Maria often uses sarcasm when talking to her friend Zoe, saying things like "Oh, sure, like you could ever do that!" Even though Maria says she's just joking, Zoe feels hurt and put down.

Discussion Questions:

1. How might Zoe feel about Maria's sarcasm?
2. How can Zoe express how she feels about these "jokes"?
3. How can friends ensure their jokes don't hurt others?

Scenario 8: Mocking Someone's Accent or Way of Speaking

Diego has a different accent because he moved from another country. Some students, including Lily, often mimic Diego's accent and laugh when he talks. Diego feels self-conscious and tries to avoid speaking in class.

Discussion Questions:

1. How do you think Diego feels when his accent is mocked?
2. What can Diego do to stand up for himself?
3. How can others support Diego and make him feel included?

TOC Title: G7 Introduction to Artificial Intelligence

Lesson Title: Introduction to Artificial Intelligence
Grade Level: 7
Duration: 45 minutes

Objective:

- The students will be able to define the term Artificial Intelligence (AI).
- The students will understand how AI impacts society and its potential future roles.

Suggested Materials:

- Whiteboard and markers.
- Pencil/pens and paper.
- Short video about AI (3–5 minutes). Suggestion: *What is Artificial Intelligence? | Artificial Intelligence In 5 Minutes | AI Explained | Simplilearn*, https://www.youtube.com/watch?v=uMzUB89uSxU (5 minutes), or a similar age-appropriate video.

Procedure

Introduction (5 minutes):

a. Whole group discussion: Ask the class how many students have used Siri, Alexa, or a smart speaker before. Ask if they have noticed how YouTube or Netflix recommends what you might like to watch next.
b. Define AI as a type of technology that allows computers and machines to learn, make decisions, and perform tasks that normally require human intelligence.
c. Emphasize that AI is not like robots from movies. It is software that allows machines to think and learn.

Discussion on Online Safety Rules (10 minutes):

a. Show a short video explaining what AI is and some of its applications in the real world. Suggestion: *What is Artificial Intelligence? | Artificial Intelligence In 5 Minutes | AI Explained | Simplilearn*, or a similar age-appropriate video.

Activity (15 minutes):

a. Ask the students to think of examples of AI they encounter daily.
    - Examples could include smart assistants (Siri, Alexa), self-driving cars, video game characters, recommendation systems (YouTube, Spotify), or Google searches.
b. Create a web on the board with “AI” in the center and students’ examples branching out.

c. Follow-up discussion questions:
  - How does AI help make our lives easier?
  - What kinds of jobs or tasks might AI do in the future?

Small Group Activity (15 minutes):

a. Divide the class into small groups (three to four students each).
b. Have each group design their own AI app. Groups should consider the following:
  - What will it do?
  - Who will it help?
  - How will it learn or improve over time?
c. Suggest ideas if groups are struggling:
  - AI that helps with homework.
  - AI that assists doctors or firefighters.
  - AI for video game development.
d. Have each group write down their idea on a piece of paper.
  - Name of their AI application.
  - Purpose: What does it do?
  - Who will benefit from it?
  - How will it learn or get better?
e. Give groups 15 minutes to come up with their idea.

Present and Discuss (10 minutes):

a. Each group presents their AI app to the class (1–2 minutes per group).
b. Discussion questions after each presentation:
  - How could this app make life easier or better?
  - What could be some challenges with making this kind of AI work?

Conclusion (5 minutes):

a. Summarize the key points:
  - AI helps machines learn and make decisions.
  - We already use AI in everyday life, and it will keep growing in the future.
  - Ask reflective questions such as:
  - hat do you think AI will look like when you're adults?"
  - hat would you want AI to do for you in the future?"

Assessment:

a. Evaluate students based on their participation in discussions and the creativity of their AI app ideas.

Grade 8

TOC Title: G8 Acceptable Behavior
Lesson Title: Acceptable Behavior
Grade Level: 8
Duration: 40 minutes

Objective:

- The students will be able to define acceptable behavior.
- The students will be able to identify acceptable and unacceptable behaviors in different environments (school, home, community).
- The students will understand the impact of acceptable behavior on relationships and personal growth.

Suggested Materials:

- Whiteboard and markers.
- Chart paper and markers.
- Scenarios for group activity (provided below).
- Notebooks and pens for journal activity.

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask students what acceptable behavior means to them.
b. Write down student responses on the whiteboard.
c. Define acceptable behavior as actions, speech, and attitudes that are considered appropriate, respectful, and responsible in different situations.
d. Explain that the focus of the lesson is to explore why acceptable behavior matters in school, at home, and in the community.

Group Activity (15 minutes):

a. Divide students into small groups (three to four per group).
b. Give each group a handout with different behavior-related scenarios.
c. Have students discuss the following:
    - Whether the behavior in the scenario is acceptable or unacceptable.
    - What the consequences of the behavior might be.
    - Could have behaved better? If so, how?
d. Each group will share one scenario and their conclusions with the class.

Journal Activity (10 minutes):

a. Ask students to reflect on their own behavior in school, at home, and in their community by writing in their notebooks.
b. As they write, they should
    - identify one behavior they are proud of,
    - identify one behavior they would like to improve, and
    - set a personal goal for how they will work on improving their behavior in one setting.

Conclusion (5 minutes):

a. Encourage students to reflect on how their actions can affect people around them.

Assessment:

b. An assessment can be taken based on participation in activities and each student's journal reflection.

Scenarios for Group Activity:

1. A teacher is explaining a new topic in class. One student keeps interrupting by talking to their friend and using their phone.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

2. You are asked to help with household chores, but you refuse and instead spend time playing video games while your sibling ends up doing your share of the work.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

3. During lunch, a group of friends starts teasing one of their classmates about their appearance. At first, it seems like a joke, but the classmate becomes visibly upset.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

4. You and a group of friends are at a local park. Some of your friends start littering and being loud, disturbing others who are trying to enjoy their time.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

5. A student posts a negative comment on social media about a classmate. Other students begin sharing and adding to the post, making fun of the classmate.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

6. During a group project, one person is not contributing and makes excuses for not doing their part. The rest of the group has to pick up the extra work.
   Is the behavior in the scenario acceptable or unacceptable?
   What might the consequences of the behavior be?
   Could the person in the scenario have behaved better? How?

7. You are riding the bus, and it is crowded. An elderly person gets on, and there are no more seats available. You remain seated while others are standing.
    Is the behavior in the scenario acceptable or unacceptable?
    What might the consequences of the behavior be?
    Could the person in the scenario have behaved better? How?

8. A group of friends is pressuring one of their classmates to skip school and go to the mall instead. The classmate feels uncomfortable but does not want to lose their friends.
    Is the behavior in the scenario acceptable or unacceptable?
    What might the consequences of the behavior be?
    Could the person in the scenario have behaved better? How?

TOC Title: G8 Ethics & Leadership

Lesson Title: Ethics & Leadership
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will be able to define ethics and leadership.
- The students will understand the importance of ethical behavior in leadership.
- The students will be able to apply ethical reasoning to real-life scenarios.

Suggested Materials:

- Chalkboard/Whiteboard.
- Chalk/Markers.
- Paper and pencils.
- Printed scenarios for group discussions (provided below).

Procedure

Introduction (10 minutes):

Whole Group Discussion:

a. Begin by asking students what they think the words ethics and leadership mean. Write down their answers on the board.
b. Explain that ethics is about knowing what's right and wrong, and making decisions is based on that understanding.
c. Explain that leadership is not just about being the boss, but about guiding others and making good decisions for everyone.
d. Discuss the role of a leader, and what ethical qualities make them a good leader (honesty, fairness, kindness).
e. Ask students for examples of leaders in their community or personal lives and what qualities they admire in them.

Activity (20 minutes) Ethical Dilemmas:

a. Divide students into small groups (three to four students per group). Provide each group with a scenario that involves a leadership or ethical dilemma. Ask them to discuss the scenario and decide what an ethical leader should do.
b. After 10 minutes, each group shares their scenario and solution with the class. Discuss as a class whether they think each group's solution was ethical and why.

Reflection and Leadership Qualities (10 minutes):

a. **Discussion:** Ask students to think about what qualities they would like to develop as future leaders.
b. **Reflection Activity:** Have students write down one ethical leadership quality they admire and one way they can demonstrate that quality in their daily lives.

Conclusion (5 minutes):

a. Recap the main points — ethics is about doing the right thing, and good leaders use ethics to guide their actions.

Assessment:

a. An assessment can be taken based on participation in group activities and discussions, and the written reflection.

Scenarios for Activity:

a. The Forgotten Homework: You forgot to do an important homework assignment. They ask if they can copy your work so they can get it turned in and not get in trouble.

b. Unfair Distribution: During a class project, one student does all the work while the others in the group do nothing. The teacher asked the group leader if everyone worked equally. What should the leader say?

c. Sports Team Favoritism: The coach of a sports team seems to be favoring certain players, giving them more opportunities to play, even though others are more skilled or have worked harder. As a team leader, what would you do to ensure fairness?

d. Bullying in the Hallway: A student is being bullied during lunch. A group of students witness it but are afraid to speak up. As a leader, what action should be taken?

e. Cheating on a Test: During an exam, a student sees their classmate cheating. They are not sure if they should tell the teacher. How would a responsible leader handle this situation?

f. Unkind Comments Online: A student finds that a classmate is posting hurtful comments about others on social media. Many students know about it but have not done anything. How would a responsible leader address this?

g. Classroom Cleanup: After a school event, some students leave without helping to clean up. The student in charge of cleaning up notices, but does not want to be disliked for making others do the work. How should they act in this situation?

h. Friend in Trouble: A student is struggling with their schoolwork but is too embarrassed to ask for help. What steps should be taken to support them?

i. Group Project Credit: A group project receives a high grade, but one of the members did little to no work. The teacher asks the group leader to verify if everyone contributed equally. What should the leader do?

j. Peer Pressure on a Trip: During a school trip, some students want to go into an area they know is off limits. The group leader knows it is wrong but fears being left out if they refuse. What should the leader do?

TOC Title: G8 Cyberbullying

Lesson Title: Cyberbullying
Grade Level: 8
Duration: 40 minutes

Objective:

- Students will be able to define cyberbullying.
- Students will understand its effects, and how to respond to it.
- Students will know and be able to use strategies to protect themselves and others from cyberbullying.

Suggested Materials:

- Internet access for showing videos.
- Whiteboard and markers.
- Printed handouts of scenarios.
- Student journals or notebooks. There are several online sites and free resources for journaling. Here is one specifically for teens that may provide journaling ideas. Grade 7 & 8 Prompts » JournalBuddies.com.
- Optional: Short video on cyberbullying. Suggestion: *Emma's Story: Cyberbullied by a Best Friend* (2 minutes 21 seconds), https://www.youtube.com/watch?v=qA1TJjJgdz8, or a similar age-appropriate video.

Procedure

Introduction (5 minutes):

a. Begin by asking students what they know about bullying and how it can happen online.
b. Write their responses on the board.
c. Introduce the concept of cyberbullying by defining it: "Cyberbullying is the use of digital devices, sites, and apps to harm or intimidate others."

Video and discussion (10 minutes):

a. Show the suggested video on cyberbullying, or another age-appropriate video that depicts cyberbullying.
b. After the video, discuss the following:
    - Examples of cyberbullying.
    - How cyberbullying makes people feel.
    - Why it is important to address cyberbullying.

Activity (20 minutes):

a. Reflection and Journaling:
  - Ask students to reflect on a time they witnessed or experienced cyberbullying. (*Note*: Emphasize that they can write about a friend's experience or create a fictional scenario if they are uncomfortable sharing personal experiences.)
  - Have them write a short journal entry on how they felt and what they think could have been done to handle the situation better.

Conclusion (5 minutes):

a. Recap the importance of being kind online and what students can do if they or someone they know is being cyberbullied.
b. Provide students with a list of resources, such as a list of international hotlines at https://blog.opencounseling.com/suicide-hotlines/.
c. Encourage them to talk to a trusted adult if they ever feel unsafe online.

Assessment:

a. Participation in group discussions and activities.
b. Quality of reflections in their journal entries.

TOC Title: G8 Disability Bullying
Lesson Title: Disability Bullying
Grade Level: 8
Duration: 40 minutes

Objective:

- The students will understand the impact of disability bullying.
- The students will know and be able to use strategies to stop or prevent disability bullying.

Suggested Materials:

- Whiteboard and markers.
- Scenarios for group activity (provided below).

Procedure

Introduction (5 minutes):

a. Watch a video that discusses disabilities. Suggestion: *Disabilities: How to Cope With Them & Support Others* (youtube.com) (2 minutes 23 seconds), or another age-appropriate video on disabilities.
b. Whole group: Start a discussion on bullying by asking students to define what bullying is.
c. Guide the discussion to the bullying of people with disabilities. Ask students why they think this happens, and how they think it affects people.
d. Encourage brief student responses and write down key points on the board.

Empathy Building Activity (10 minutes):

a. Randomly pair students up. Give pairs 3 minutes to discuss two things they have in common and two things that make them different.
b. After pairs share with each other, ask for a few volunteers to share with the class.
c. Relate this back to the concept that we all have things that make us unique, but those differences do not make any of us less valuable or worthy of respect.
d. Briefly explain that some differences, like disabilities, can be misunderstood which sometimes leads to bullying.

Activity: Role-Playing Scenarios (20 minutes):

a. Divide students into small groups.
b. Give each group a bullying scenario related to disability. Ask them to come up with a solution that focuses on how they would stand up for the person being bullied or prevent the bullying.

c. Groups should address the following:
  - What is wrong in this scenario?
  - Why do they think it is happening?
  - What positive solution(s) can they come up with to help the victim and build a more understanding community?

d. After 10 minutes, have each group either act out their scenario or share their solution with the class.

Conclusion (5 minutes):

a. Reinforce the key message that we are all different in some way, but everyone deserves respect. We can stand up for others and we should always promote kindness.

b. Encourage students to think about what they can do each day to make their school a more inclusive and respectful place for everyone.

Assessment:

a. An informal assessment can be taken based on students' participation in discussions and role-playing activities.

Scenarios for Role-Playing Activity:

Scenario 1: Exclusion During Recess

A student with a mobility challenge is sitting by the side of the playground during recess. Other students are playing a running game but don't invite the student to join in. Some kids whisper and glance at the student but don't include them.

Scenario 2: Teasing for Extra Help

A student with a learning disability needs extra time and assistance to finish assignments. Another student starts making jokes about how slow they are, and others laugh along. The student looks upset and embarrassed but stays silent.

Scenario 3: Mocking Sensory Needs

A student with a sensory sensitivity wears noise-canceling headphones during a loud school event. Another student points it out, and others start mocking the student, calling the headphones "weird" and making loud noises near them on purpose.

Scenario 4: Disability and Sports

A student with a physical disability wants to join a basketball game, but others claim it will "slow down the team" or say that it's "too difficult" for them to participate. The student looks discouraged but doesn't say anything.

Scenario 5: Cyberbullying

A student with a disability posts a photo on social media, and someone leaves a mean comment related to their appearance or disability. Other students see the comment but don't know what to do.

Scenario 6: Unkind Nicknames

A student with a speech impediment is given an unkind nickname by some students because of the way they talk. Others start using the nickname, not realizing how hurtful it is. The student feels uncomfortable but doesn't speak up.

Scenario 7: Ignoring in Group Work

During a group project, a student with a visual impairment suggests an idea, but other group members ignore the suggestion and talk over the student. The student starts to withdraw and stops participating.

Scenario 8: Making Fun of Assistive Devices

A student uses a communication device to help them speak, and other students make fun of the robotic voice the device uses. They start mimicking the voice, causing the student to feel embarrassed.

TOC Title: G8 Emotional Bullying
Lesson Title: Emotional Bullying
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will understand what emotional bullying is and the effects it has on people.
- The students will know and be able to use strategies for addressing emotional bullying as both victims and bystanders.

Suggested Materials:

- Whiteboard/markers.
- Paper and pens.
- Premade scenario cards (provided below).

Procedure

Introduction to Emotional Bullying (10 minutes):

a. Whole group: Define emotional bullying: When someone uses words, threats, or exclusion to harm someone's feelings or self-worth. Examples include name-calling, spreading rumors, exclusion from groups, and manipulation.
b. Discussion: Ask the class if they have seen or heard about emotional bullying before (in media, school, etc.).
c. Effects: Discuss the emotional impact of this type of bullying (anxiety, depression, social isolation, low self-esteem).

Group Activity: Identifying Emotional Bullying (15 minutes):

a. Divide students into small groups (three to four students per group). Give each group a scenario card. Each card describes a situation involving emotional bullying (e.g., a group spreading rumors, exclusion at lunch, or online name-calling).
b. Each group responds to the following prompts:
    - Identify the emotional bullying behavior.
    - Discuss how they think the victim might feel.
    - Share ideas on what bystanders or friends can do to support the victim.
c. After 10 minutes (or once all groups are finished), bring the class back together and ask groups to share their scenario and their response.

Teacher-led Discussion: Strategies for Dealing with Emotional Bullying (15 minutes)

a. As a Victim:
  - Don't Respond with Anger: Reacting with anger can escalate the situation.
  - Tell Someone You Trust: A teacher, counselor, another trusted adult, or friend.
  - Practice Self-care: Focus on building self-esteem and finding supportive friendships.
  - Assertively Stand Up for Yourself: Teach students "I" statements (e.g., "I don't appreciate being spoken to that way.").

b. As a Bystander:
  - Speak Up: If it is safe, tell the bully to stop.
  - Support the Victim: Sit with them, talk to them, make sure they know they're not alone.
  - Report the Bullying: Report the bullying to a trusted adult.
  - Be Kind: Even small acts of kindness help.

Conclusion (5 minutes):

a. Ask students to think of one thing they learned about emotional bullying today and one thing they can do if they witness it in the future. Invite volunteers to share their thoughts.

b. Reinforce that emotional bullying is harmful but can be addressed through kindness, support, and taking action.

Assessment:

a. Informally assess each student's participation in group discussions and role-plays.

Scenarios for Group Activity:

Scenario 1: Exclusion at Lunch

During lunch, a group of students decides not to let another student sit with them. Every day, they make excuses about why there's no room at the table or why the person can't join them.

- Identify the emotional bullying behavior.
- How might the person who is excluded feel?
- What can bystanders do to help in this situation?

Scenario 2: Online Name-Calling

A student posts a picture of themselves on social media. Others start leaving mean comments about the way they look, making fun of their clothes and appearance. The comments keep coming, and some people join in even though they aren't close friends.

- Identify the emotional bullying behavior.
- How might the victim feel after seeing these comments?
- What can a bystander do in this situation?

Scenario 3: Rumor Spreading

A student tells a secret to a close friend. The next day, everyone in school knows the secret, and people start spreading rumors, adding details that are not true. The student who shared the secret feels embarrassed and hurt.

- Identify the emotional bullying behavior.
- How might the student whose secret was shared feel?
- How should bystanders react when they hear the rumor?

Scenario 4: Manipulating Friendships

A group of students tells another student that they won't be their friend anymore unless they stop talking to someone else. The student feels pressured to choose between friendships.

- Identify the emotional bullying behavior.
- How might the student being manipulated feel?
- What could a bystander or the victim do to handle this situation?

Scenario 5: Public Humiliation

In class, a student accidentally answers a question wrong. Other students laugh and start calling the person “stupid” or “dumb” for the rest of the day. The teasing continues, and it becomes an inside joke among classmates.

- Identify the emotional bullying behavior.
- How might the student being teased feel?
- What could a bystander do in this situation to help?

Scenario 6: Social Media Exclusion

A group of students creates a group chat online, but they purposely leave one student out. They talk about things they are doing together and make inside jokes. The excluded student finds out and feels hurt.

- Identify the emotional bullying behavior.
- How might the excluded student feel?
- How could a bystander help the student left out?

Scenario 7: Making Fun of Personal Interests

A student shares their love for a particular hobby, like reading comic books or playing video games. Some classmates start teasing them, saying the hobby is “lame” or “childish.” They make fun of the student every time the hobby is mentioned.

- Identify the emotional bullying behavior.
- How might the student feel being made fun of for their interests?
- What can bystanders do to stop the teasing?

TOC Title: G8 Personal Bullying

Lesson Title: Personal Bullying
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will be able to define and recognize personal bullying.
- The students will understand the harmful effects of personal bullying on individuals and communities.
- Develop empathy by recognizing how bullying affects mental health and self-esteem.
- The students will know and be able to use strategies to prevent/stop bullying.

Suggested Materials:

- Whiteboard/Smartboard.
- Markers.
- Handouts with scenarios and discussion questions.
- Spiral notebook for journaling. There are several online sites and free resources for journaling. Here is one specifically for teens that may provide journaling ideas. Grade 7 & 8 Prompts » JournalBuddies.com.

Procedure

Introduction (10 minutes):

a. Whole group: Ask students to describe what bullying means.
b. Write students' ideas on the board.
c. Explain that personal bullying refers to targeting someone because of their gender or sexuality.

Wrap up the introduction discussion by emphasizing that

- bullying based on gender identity or sexuality is harmful because it attacks an important part of who a person is;
- it can lead to serious consequences, like anxiety, depression, or even self-harm in extreme cases.

Activity — Building Empathy (15 minutes):

a. Divide the class into small groups and give each group a scenario where personal bullying might occur.
b. Ask groups to
    - act out the scenario,
    - discuss how the person being bullied might feel, and
    - come up with positive ways bystanders could intervene and support the bullied person.

Debrief & Reflection (10 minutes):

a. Discuss the following:
  - How can bullying affect someone's mental health and sense of self-worth?
  - How does this kind of bullying affect our community?
  - What would you do if you saw someone being bullied because of their gender or sexuality?

b. Key Discussion Points:
  - Encourage empathy by asking students how they would feel in the victim's shoes.
  - Explore ways to be an upstander, including reporting bullying, supporting the victim, and speaking out against harmful behavior.
  - Ensure that students understand that bullying harms the mental health of victims and bystanders, disrupts the school environment, perpetuates division, and erodes trust.

Journaling Activity (10 minutes):

a. Encourage personal reflection on the lesson and reinforce understanding of empathy, respect, and taking action against bullying.

b. At the end of the lesson, ask students to take 10 minutes to reflect on the lesson in a journal. Let them know their responses will remain private unless they choose to share. This encourages honest, personal reflection.

c. Offer the following prompt as a suggestion but allow students to write about anything they are thinking about related to the lesson.
  - Suggested prompt: Why is it important to respect people's gender identities and sexual orientations, even if they are different from your own? How can respecting others make your school a better place?

d. Encourage students to continue journaling as a way to reflect on issues that concern them, or as a way to help process their thoughts and feelings.

Conclusion (5 minutes):

a. Review discussion and activity topics from the lesson.

Assessment:

e. An informal assessment can be taken based on participation in discussions and activities.

Suggested Scenarios for Role-Playing Activity:

1. A student is teased for dressing in a way that doesn't align with traditional gender norms.

2. Someone overhears classmates making fun of a peer for liking someone of the same gender.

3. A group of students excludes someone because of their gender identity.

4. A classmate posts a picture on social media expressing pride in being part of the LGBTQ+ community. In response, some students leave mean comments like "You're just doing it for attention" and "That's gross."

5. A rumor starts spreading around school that a student might be gay because they haven't dated anyone of the opposite gender. Soon, students start whispering and pointing at them in the hallways, making jokes behind their back.

6. During gym class, one student is teased and pushed around in the locker room because they don't fit into typical gender norms. Some students make hurtful comments about their body, calling them names and saying they don't belong in either locker room.

7. A classmate has two moms, and when they mention this during a class discussion about family, some students start whispering and giggling. A few students make comments like "That's not a real family," and the student feels embarrassed and upset.

TOC Title: G8 Physical Bullying

Lesson Title: Physical Bullying
Grade Level: 8
Duration: 45 minutes

Objective:

- Students will be able to define physical bullying.
- Students will know and be able to use strategies to prevent or stop physical bullying.
- Students will understand the importance of standing up against bullying and supporting their peers.

Suggested Materials:

- Whiteboard and markers.
- Role-play scenario cards (suggested scenarios included below).

Procedure

Introduction (10 minutes):

a. Full group discussion: Ask students what bullying is, and what types of bullying they know about. Write down their answers on the board.
b. Explain that bullying can there are several types of bullying. In this lesson, we will focus on physical bullying (hitting, pushing, damaging belongings, etc.).
c. Ask students how they think someone feels when they are being physically bullied. What might prevent them from asking for help?
d. Brainstorm some ways to prevent physical bullying from occurring. Encourage students to think about actions they can take as individuals, as a class, and as a school community.

Key Strategies to Prevent and Stop Physical Bullying (10 minutes):

Share the following strategies:

a. **Speak Up:** Encourage students to speak up if they see bullying happening, whether by telling a teacher or directly telling the bully to stop (if safe).
b. **Support the Victim:** Be a friend to the person being bullied. This could mean walking with them, offering kind words, or just listening.
c. **Involve Adults:** Emphasize the importance of telling a trusted adult, like a teacher, counselor, or parent, if they see or experience bullying.
d. **Set a Good Example:** By being kind and respectful, students can create a positive environment where bullying is less likely to happen.
e. **Create Safe Spaces:** Encourage forming peer support groups or anti-bullying clubs.

Role-Playing Activity (15 minutes):

Divide the class into small groups and give each group a scenario card depicting a bullying situation.

a. Role-Play: Have each group act out their scenario (suggested scenarios included below), including a resolution where students intervene in a positive way.
b. Debrief: Discuss each scenario as a class, highlighting what was done well and other possible strategies that could have been used.

Reflection and Action Plan (5 minutes):

a. Reflection: Ask students to reflect silently on a time they saw bullying or were bullied and what they wish had been done differently.
b. Action Plan: Have students write down one specific action they will take if they see physical bullying.

Conclusion (5 minutes):

a. Summarize key points of the lesson.
b. Open the floor for any questions or comments.

Assessment:

a. Student participation in the discussions and role-playing activities. The student action plans can be collected and reviewed to gauge understanding.

Suggested Scenarios for Role-Playing Activity:

Scenario 1: The Hallway Shove

Situation:
A group of students is walking down the hallway. One student, Sam, accidentally bumps into another student, Jake, who is known for bullying others. Jake shoves Sam hard against the lockers and laughs, making fun of Sam in front of everyone.

Roles:

- Sam (victim): The student who got pushed.
- Jake (bully): The student who did the pushing.
- Bystanders: Friends of Sam who witnessed the incident.

Goal:
Bystanders should practice speaking up, supporting Sam, and getting a teacher if necessary. Explore different ways to handle the situation without escalating it.

Scenario 2: Lunchroom Trouble

Situation:
During lunch, Emma, a quiet student, is sitting alone. A group of students walks by and one of them, Alex, grabs Emma's lunch tray and throws her food on the floor, laughing and encouraging others to join in.

Roles:

- Emma (victim): The student whose lunch was ruined.
- Alex (bully): The student who threw the lunch.
- Bystanders: Students who are sitting nearby and saw what happened.

Goal:
Bystanders should practice comforting Emma, confronting Alex calmly, or alerting a lunch supervisor. Discuss how to support Emma without making the situation worse.

Scenario 3: The Playground Push

Situation:
During a break, a group of students is playing basketball. One student, Jordan, gets upset when they miss a shot and pushes another student, Taylor, to the ground in frustration. Jordan starts calling Taylor names, and a few others laugh.

Roles:

- Jordan (bully): The student who pushed and called names.
- Taylor (victim): The student who was pushed.
- Bystanders: Other students playing basketball who saw what happened.

Goal:
Bystanders should practice checking on Taylor, telling Jordan to stop, and getting an adult involved if needed. Discuss ways to calm the situation and keep the game fair.

Scenario 4: On the Bus

Situation:
On the bus ride home, Mia is sitting in her seat when Liam, a student known for bullying, starts hitting the back of her seat repeatedly and making mean comments about her. Other students are watching but unsure what to do.

Roles:

- Mia (victim): The student being bullied on the bus.
- Liam (bully): The student hitting the seat and making mean comments.
- Bystanders: Other students on the bus.

Goal:
Bystanders should role-play different responses, such as moving to sit with Mia, telling Liam to stop, or informing the bus driver. Discuss the importance of not ignoring the bullying.

Scenario 5: Gym Class Intimidation

Situation:
In gym class, a student named Chris is not good at dodgeball and gets hit often. A group of students led by Ryan starts targeting Chris, throwing balls at him harder than necessary and taunting him about his lack of skills.

Roles:

- Chris (victim): The student being targeted during dodgeball.
- Ryan (bully): The leader of the group targeting Chris.
- Bystanders: Other students in gym class.

Goal:
Bystanders should practice intervening by encouraging fair play, checking on Chris, and reporting the incident to the gym teacher. Discuss the importance of inclusivity in sports and not allowing bullying to happen during games.

TOC Title: G8 Racial Bullying
Lesson Title: Racial Bullying
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will understand what racial bullying is and how it differs from other types of bullying.
- The students will understand the impact of racial bullying on individuals and communities.
- The students will know and be able to use strategies to stand up against racial bullying, as a target, bystander, and ally.

Suggested Materials:

- Whiteboard and markers.
- Scenario cards (provided below).

Procedure

Introduction (10 minutes):

a. Begin with a whole group discussion on what bullying means.
b. Guide discussion to the different types of bullying, including physical, verbal, and cyberbullying.
c. Introduce the term racial bullying. Define it as bullying someone because of their race, ethnicity, or cultural background.
d. Write the definition for Racial Bullying on the board: Any behavior intended to hurt, intimidate, or belittle someone based on their race or ethnic background. This can include racial slurs, stereotypes, exclusion, or threats. This happens in person and online.

Activity: Think-Pair-Share Scenario Analysis (20 minutes):

Think (5 minutes):

a. Provide each student with a scenario card describing a situation of racial bullying. Each student should have the same scenario as one other student for the **Pair** activity.
b. Ask students to individually reflect on the scenario with the following instructions:
    - How do you think the target feels in this situation?
    - What could be the long-term impact of this kind of bullying on the person?
    - What would you do as a bystander or ally in this situation?

Pair (5 minutes):

a. Each student then pairs up with the other person with the same scenario. Pairs discuss their reflections with a partner. Each pair should
  - share their thoughts on how the target might feel and what they believe the right course of action should be; and
  - compare their ideas for how to stand up against the bullying, whether as a target, bystander, or ally.

Share (10 minutes):

a. After discussing in pairs, have a class-wide discussion. Invite several pairs to share:
  - How would you handle the situation?
  - What strategies would work best to stop the racial bullying and support the target?

b. As students share, write key points and strategies on the board (e.g., speaking up, seeking help from a teacher, supporting the target).

Empowerment Strategies (10 minutes):

a. Introduce strategies that students can use to stand up against racial bullying, either as a target, bystander, or ally. Write these on the board:
  - For the target:
    i. Assertively tell the bully to stop.
    ii. Seek help from a trusted adult or authority figure.
  - For the bystander:
    i. Speak up when you witness racial bullying. Say something like "That's not okay" or "Please stop."
    ii. Support the target — be their friend, and show solidarity.
    iii. Report the incident to a teacher or counselor.
  - For the ally:
    i. Educate others about the harm of racial bullying.
    ii. Create a culture of inclusivity in your friend group by welcoming diverse perspectives and experiences.

Conclusion (5 minutes):

a. Ask students to reflect on the following:
  - How can we create a more inclusive and respectful school environment?
  - What actions will you take moving forward if you witness or experience racial bullying?

Assessment:

a. Participation in group activities and discussions.

b. Informal evaluation through observation of students' understanding of the material.

Scenarios for Think-Pair-Share Activity:

a. Scenario 1: A student is constantly mocked by their peers for their accent during class presentations. Even when they try their best, other students laugh or mimic the way they speak.

b. Scenario 2: During lunch, a group of students makes jokes about another student's traditional clothing, calling it "weird" and refusing to sit with them.

c. Scenario 3: A student is excluded from a group project because of their race. When they ask to join, the group members make excuses, saying there isn't enough space or that their input isn't needed.

d. Scenario 4: A student overhears a racial slur being used in the hallway against someone from a different background. Other students nearby laugh or pretend not to hear it.

e. Scenario 5: In gym class, a student is intentionally left out during team selection because of their skin color. Other students whisper and exchange looks, making the student feel isolated.

f. Scenario 6: During a discussion in class, a student shares a personal story related to their culture. Later, another student mocks the story, calling the culture "strange" and making stereotypical remarks.

g. Scenario 7: A student posts a picture on social media celebrating their cultural holiday. Several classmates leave negative comments, making fun of the celebration and saying it's "not a real holiday."

h. Scenario 8: In the cafeteria, a student brings a lunch that reflects their cultural heritage. A group of students makes fun of the food, calling it "gross" and telling the student not to eat near them.

i. Scenario 9: A student is repeatedly called racial slurs during a sports game. The other team members laugh and tell the student they're just "joking around," but the comments make the student uncomfortable.

j. Scenario 10: During class discussions, one student's opinions are frequently dismissed or ignored by their peers because they come from a different cultural background. Other students roll their eyes or talk over the student.

k. Scenario 11: While walking home from school, a group of students mocks another student by mimicking their cultural gestures or making offensive imitations of their language.

l. Scenario 12: In art class, a student draws a picture representing their cultural identity. Other students laugh at the drawing, calling it “weird” and saying that it doesn’t belong in their project.

m. Scenario 13: A student’s family recently moved from another country, and they are struggling to adjust. Other students avoid them, saying things like “You don’t belong here,” or making fun of their unfamiliarity with certain customs.

n. Scenario 14: During a class discussion on history, a student shares pride in their cultural heritage. A classmate makes a comment under their breath, saying something negative about the student’s country or ethnic group.

o. Scenario 15: At a school assembly, a student of a different race is sitting alone. Other students make a point to sit far away, whispering and pointing at the student as they laugh.

p. Scenario 16: In a group chat, some students share memes and jokes that are based on harmful racial stereotypes. One student speaks up to say it’s offensive, but the others tell them to “stop being so sensitive.”

TOC Title: G8 Religious Bullying

Lesson Title: Religious Bullying
Grade Level: 8
Duration: 45 minutes (47 minutes with video)

Objective:

- Students will be able to define religious bullying.
- Students will understand the impact of religious bullying
- Students will know and be able to use strategies to prevent religious bullying.

Suggested Materials:

- Whiteboard and markers.
- Printed handouts (or digital copies if available).
- Index cards.
- Pens or pencils.

Procedure

Introduction (10 minutes)

1. Show a short, age-appropriate video that depicts a scenario of physical bullying suggestion: Stoughton Teen Bullied For Weight, Religion Shares His Story (youtube.com) (2 minutes).
2. Explain that today's lesson will focus on understanding religious bullying, its effects, and how to prevent it.
3. Ask students if they know what bullying is and if they've heard of religious bullying.
4. Provide a clear definition: Religious bullying is treating someone badly because of their religious background or beliefs, making negative comments about a religious background or belief, calling someone names, or telling jokes based on his or her religious beliefs to hurt them.
5. Share age-appropriate examples of religious bullying, e.g., making fun of someone's religious clothing, mocking religious practices, or excluding someone because of their beliefs.

Activity (15 minutes): Bullying Scenarios

1. **Divide the class into small groups (3-4 students).**
   a. Give each group an index card with a scenario involving religious bullying.
   b. Ask each group to discuss how the person being bullied might feel and how they might react if they were the victim, and if they were a bystander.

2. **Sharing and Reflection:**
    a. Have each group share their scenario and discussion points.
    b. Discuss as a class the common feelings and reactions people might have when they experience bullying.

Follow Up (15 minutes): Creating a Respectful Environment

1. **Brainstorming:**
    a. Ask students to think of ways to create a more respectful and inclusive classroom environment, e.g., celebrate differences, speak up about bullying, show kindness and respect toward everyone, take time to learn about others, etc.
    Write their ideas on the whiteboard.
2. **Commitment:**
    a. Have students write down one action they will take to prevent religious bullying and promote respect, e.g., Speak up, offer support to the victim, report the bullying, etc.
    b. Collect the cards and create a classroom commitment poster to display.

Conclusion (5 minutes):

- Summarize the key points of the lesson.
- Emphasize that everyone has a right to feel safe and accepted. Religious beliefs should not be a factor.

Assessment:

a. An informal assessment can be taken based on student participation and contribution to discussions and activities.

Scenarios for Group Activity:

Scenario 1: A student named Ali wears a headscarf to school every day as part of her religious practice. Some classmates start calling her names and making fun of her headscarf during lunch.
Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 2: During a history lesson, a student named Sam shares that he doesn't eat certain foods due to his religious beliefs. Another student loudly mocks him and says his religion is weird.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 3: Maria recently moved to the area and practices a different religion than most of her classmates. When she invites a few classmates to her religious festival, they laugh and tell her they don't want to attend her "weird" event.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 4: During a holiday season, a student named David talks about his family's traditions. Some students laugh and say his traditions are stupid because they don't celebrate in the same way.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 5: In a group project, a student named Ravi needs to leave early on Fridays for his religious services. His group members complain and say he's just trying to get out of work.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 6: A new student, Leila, wears a religious symbol around her neck. A few classmates point at it, whisper to each other, and giggle every time she walks by.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 7: During a class discussion, a student named Ahmed shares a story from his religious text. Some students roll their eyes and one says, "No one cares about your religion."

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 8: A student named Ethan is teased because he doesn't participate in certain school activities due to his religious beliefs. His classmates call him boring and make him feel left out.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 9: A group of students starts spreading rumors about Sarah, saying her family does strange things at home because of their religion. They laugh about it and refuse to sit with her at lunch.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

Scenario 10: During a field trip, a student named Juan prays quietly before eating lunch. Some classmates notice and start imitating him in a mocking way, making him feel embarrassed.

Discussion points:

- What is happening in this scenario?
- How might the victim feel?
- How might you react in this scenario as the victim? As a bystander?

TOC Title: G8 Social Bullying
Lesson Title: Social Bullying
Grade Level: 8
Duration: 40 minutes

Objective:

- The student will understand what social bullying is and its different forms.
- The students will recognize the impact of social bullying on individuals and communities.
- The students will know and be able to use strategies to prevent and respond to social bullying.

Suggested Materials:

- Whiteboard/markers.
- Chart paper and markers (for group work).
- Paper slips for exit activity.

Procedure

Introduction (10 minutes):

a. "Whole group: Ask students what they think of when they hear the term 'bullying'?" Encourage a brief class discussion.
  - Define Social Bullying:

    Explain that social bullying involves damaging someone's reputation, relationships, or social status. This can happen through exclusion, gossip, public humiliation, or spreading rumors. This can happen online as well.

Discussion (15 minutes):

a. Provide real-life examples of social bullying (e.g., gossiping, exclusion from groups, spreading false rumors, and cyberbullying through social media).
b. Discuss how these behaviors harm others emotionally and socially.
c. Write the following categories on the board:
  - Gossip
  - Exclusion
  - Spreading Rumors
  - Public Humiliation.

Ask students to give specific examples under each category. Engage the class by discussing how each type of behavior could make someone feel.

Activity: Prevention (10 minutes):

a. As a class brainstorm ways to prevent social bullying in their school community.
b. Suggest additional ideas to supplement student ideas:
   - Reporting bullying to a trusted adult.
   - Including others in conversations or activities.
   - Standing up for others in nonconfrontational ways.
   - Starting an anti-bullying campaign or club in school.

Conclusion (5 minutes):

a. Exit Slip Activity.
b. Give each student an exit slip with the prompt.
c. "What will you do if you see someone being socially bullied? What can you do to stop social bullying in your school?"
d. Students should write their responses and submit them before leaving.

Assessment:

a. Participation in group activity and role-playing.
b. Reflection on exit slips.
c. Observation of class discussion and engagement.

TOC Title: G8 Verbal Bullying

Lesson Title: Verbal Bullying
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will understand the impact of verbal bullying.
- The students will know and use strategies to counter verbal bullying.
- The students will develop leadership skills to promote a positive school environment.

Suggested Materials:

- Whiteboard and markers.
- Index cards and pens.
- Scenario cards (provided below).

Procedure

Introduction (5 minutes):

a. Whole group discussion: Ask students what they think verbal bullying is. Write key terms on the board (e.g., teasing, name-calling, rumors).
b. Briefly define it and its effects, emphasizing how it impacts both the victim and the community.

Understanding the Impact (15 minutes):

a. Empathy Exercise.
    - Distribute index cards and ask students to write down a time when words hurt them or when they witnessed verbal bullying. Let students know that the cards will be read to the class for discussion, but names will not be used.
    - Collect cards anonymously and read a few aloud (ensuring they're appropriate).
b. Group Reflection
    - Discuss how these experiences might feel. Highlight the emotional impact, including anxiety, sadness, and isolation.

Leadership Activity (20 minutes):

a. Divide the class into small groups and give each group a verbal bullying scenario (suggestions provided below).
b. Each group will come up with a plan that responds to the following questions. How can you support the victim? How can you stop the bullying behavior without escalating the situation? How can you involve others to help?
c. Groups present their action plans to the class.
d. Lead the class in a positive discussion on each group's plan.

Conclusion (5 minutes):

a. Whole group: Ask students what they learned about verbal bullying, and how good leadership can help prevent it.

Assessment:

a. Make an informal assessment based on student participation in discussions and activities.

Scenarios for Activity:

1. A student in your class is repeatedly called names like "nerd" and "loser" by a group of students whenever they answer questions in class. They are starting to stay quiet and are reluctant to participate in class activities.
   How can you support the victim?
   How can you stop the bullying without escalating the situation?
   How can you involve others to help?

2. Someone started a false rumor about your friend that they cheated on a test. Now, everyone in school is talking about it, and your friend is upset and feels isolated.
   How can you support the victim?
   How can you stop the bullying behavior without escalating the situation?
   How can you involve others to help?

3. Classmates have teased a friend about her clothes and appearance, with comments like "Why do you always wear the same stuff?" and "You look so weird." Your friend tries to laugh it off but is clearly hurt.
   How can you support the victim?
   How can you stop the bullying behavior without escalating the situation?
   How can you involve others to help?

4. A group of students created a group chat where they made fun of another student by sharing mean jokes and negative comments about his posts on social media. He found out and is devastated.
   How can you support the victim?
   How can you stop the bullying without escalating the situation?
   How can you involve others to help?

5. During lunch, a group of students always tells one girl that she can't sit with them because "there's no space" or "this table is full." She often ends up sitting alone, feeling left out.
   How can you support the victim?
   How can you stop the bullying behavior without escalating the situation?
   How can you involve others to help?

6. During a group project, one student is constantly put down by her group members with comments like “Your ideas are stupid” and “You’re not smart enough to do this part.” As a result, she is losing confidence and isn’t contributing anymore.
   How can you support the victim?
   How can you stop the bullying behavior without escalating the situation?
   How can you involve others to help?

7. On the school’s basketball team, teammates constantly tease one player for missing shots during practice. Comments like “You’re the worst player on the team” and “We’d be better off without you” are thrown around regularly.
   How can you support the victim?
   How can you stop the bullying behavior without escalating the situation?
   How can you involve others to help?

8. A quiet student is often ignored or talked over by classmates during discussions or group work. When she tries to contribute, some students roll their eyes or sigh loudly, sending a clear message that her input isn’t welcome.
   How can you support the victim?
   How can you stop the bullying without escalating the situation?
   How can you involve others to help?

TOC Title: G8 Ethics and Artificial Intelligence
Lesson Title: Ethics and Artificial Intelligence
Grade Level: 8
Duration: 45 minutes

Objective:

Suggested Materials:

- Whiteboard and markers
- Printed handouts with scenarios (provided below)
- Exit slips for conclusion (provided below)
- Short video (optional). Suggestion: How AI tools like ChatGPT are changing homework | CBC Kids News https://www.youtube.com/watch?v=HGaO-s4AtGY 5 min. 16 sec.

Procedure

Introduction (10 Minutes)

a. Whole group discussion: Ask class what they know about Artificial Intelligence. Ask for examples of AI we interact with (examples might include: Siri, Alexa, Google, TikTok algorithms, self-driving cars, facial recognition, etc.). Write down responses on the whiteboard. Discuss briefly and clarify what AI is. Clarify that AI refers to machines designed to mimic human intelligence and perform tasks like decision-making, speech recognition, and language translation.
b. Optional Video: Show a short video on the ethics of using AI.

Suggestion: How AI tools like ChatGPT are changing homework | CBC Kids News.

Exploring the Ethical Dilemmas of AI (10 minutes)

a. Class Discussion (5 minutes): Start by asking class how AI can make our lives easier. Ask if they think it is always fair and ethical.
b. Guide the discussion toward key concerns like:
    i. Bias and Discrimination: AI can inherit human biases (e.g., facial recognition systems misidentifying certain races).
    ii. Privacy Concerns: AI systems often collect large amounts of data, raising concerns about surveillance and data misuse.
    iii. Job Automation: AI replacing human workers in industries like manufacturing and customer service.
    iv. Autonomy and Decision-Making: How comfortable are we letting AI make critical decisions (e.g., in medicine or driving)?

Activity: AI Ethics Scenarios (15 minutes)

a. Divide class into small groups (3-4 students each) and give each group a scenario (provided) that involves AI with ethical dilemmas.
b. Each group should discuss the ethical problems in their scenario and propose a solution or recommendation.
c. Discussion Prompts:
    i. What is the ethical issue in your scenario?
    ii. Who benefits and who might be harmed?
    iii. Can the AI be improved to avoid the issue? How?
d. Each group shares their scenario and solution with the class (about 1–2 minutes per group).

Creating AI Guidelines (5 minutes)

Summarize what has been learned and establish guidelines for ethical AI use.

a. On the whiteboard, write: "What makes AI ethical?"
b. Ask students to contribute ideas to create a class list of "AI Ethics Guidelines." Example guidelines might include:
    i. AI should treat everyone fairly.
    ii. AI should respect privacy and data security.
    iii. AI should not replace humans in roles that require empathy or critical human judgment.
    iv. AI should be transparent in how decisions are made.

Conclusion (5 minutes):

a. Summarize key points from the lesson.
b. Hand out exit slips.

Assessment:
Assessment can be based on student participation in group discussions and presentations, and the quality of the responses on the exit slips.

Scenarios for Activity:

AI in Hiring

A large company uses an AI program to screen job applicants. However, after a while, it is discovered that the program has a bias toward selecting male candidates over female candidates for technical roles.

Ethical Dilemma: Is it fair to let AI make decisions about hiring? How can the company ensure the AI is fair and unbiased?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

Self-Driving Cars

A self-driving car is programmed to minimize harm in case of an accident. In a sudden emergency, the car must choose between hitting a pedestrian or swerving into a barrier and injuring its passengers.

Ethical Dilemma: How should the AI make decisions about life and death? Whose safety should be prioritized?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

Surveillance AI

A city introduces facial recognition AI at public places like parks and malls to prevent crime. While it helps reduce crime rates, some people worry it invades privacy, especially when innocent people are mistakenly identified.

Ethical Dilemma: Is public safety more important than individual privacy? Should there be limits to the use of AI surveillance?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI in Social Media

Social media platforms use AI to recommend content to users, showing posts that get the most engagement (likes, comments, shares). Unfortunately, the AI tends to promote sensational or false information, as these posts get more reactions.

Ethical Dilemma: Is it ethical for social media companies to use AI that may spread misinformation just to increase user engagement?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI and Healthcare

An AI program is used by hospitals to diagnose patients based on their symptoms. It can quickly and accurately diagnose common diseases but occasionally makes errors when dealing with rare conditions, leading to incorrect treatment.

Ethical Dilemma: Should doctors rely on AI for medical decisions? Who should be responsible if the AI makes a mistake?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI and Law Enforcement

Police departments start using AI algorithms to predict where crimes are likely to happen, focusing their patrols in certain neighborhoods. However, some argue that the AI unfairly targets minority communities, leading to more arrests there.

Ethical Dilemma: Is it fair to use AI in law enforcement if it might lead to biased policing? How can fairness be ensured?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI in Education

A school uses an AI grading system to mark student essays. The AI can grade assignments quickly but sometimes penalizes students who write creatively, as it struggles to understand non-standard responses.

Ethical Dilemma: Should AI have the final say in grading students' work? What happens if AI misunderstands a student's answer?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI and Art Creation

A company creates an AI that can generate realistic paintings and music, even replicating the styles of famous artists. Some artists argue that this AI takes away their jobs and steals their creative style without permission.

Ethical Dilemma: Should AI be allowed to create art? Is it fair to the artists whose styles it mimics?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

AI in Shopping Recommendations

Online retailers use AI to recommend products to customers based on their browsing and purchase history. Sometimes, the AI suggests expensive items or even products that people do not need, causing them to overspend.

Ethical Dilemma: Is it ethical for companies to use AI to encourage more purchases, even if it leads to overspending?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

Deepfake AI

An AI program is used to create realistic "deepfake" videos that can make it look like someone is saying or doing something they never actually did. While it is used for fun in some cases, others use it for harmful purposes like spreading false information about politicians.

Ethical Dilemma: Should deepfake technology be regulated or even banned? How can we prevent its misuse?

What is the ethical issue in your scenario?
Who benefits and who might be harmed?
Can the AI be improved to avoid the issue? How?

Exit Slips – For Students

1. What is one ethical issue with AI that you find interesting?
2. If you could design your own AI, what would it do, and how would you make sure it is ethical?

Notes

1 Weber, M., et al., 2012, “The Role of a Good Character in 12-Year-Old School Children: Do Character Strengths Matter in the Classroom?” *Child Indicators Research*, 5, 317–334. https://doi.org/10.1007/S12187-011-9128-0, retrieved May 1, 2024.

2 The Center for Creative Leadership, 2024, “Direction+Alignment+Commitment (DAC)=Leadership,” The Center for Creative Leadership (CCL), www.ccl.org/articles/leading-effectively-articles/make-leadership-happen-with-dac-framework, retrieved July 2024.

3 Figure 1.1 Drawn by authors based upon material presented in The Center for Creative Leadership, 2024, “Direction+Alignment+Commitment (DAC)=Leadership,” The Center for Creative Leadership (CCL), www.ccl.org/articles/leading-effectively-articles/make-leadership-happen-with-dac-framework, retrieved July 2024.

4 Lavery, S., & Coffey, A., 2021, “Middle School Students’ Views about Leaders and Leadership,” *Improving Schools*, 24(2), 152–164. https://doi.org/10.1177/1365480220943313, retrieved July 2024.

5 WorldStrides, February 22, 2024, “10 Ways Your Middle Schooler Can Gain Leadership Experience,” www.envisionexperience.com/blog/10-ways-your-middle-schooler-can-gain-leadership-experience#:~:text=Leadership%20experience%20in%20middle%20school,on%20personal%20growth%20and%20success.

6 Haynes-Tross, E., 2015, “The Importance of Developing Leadership Skills in Grades 6–8 Middle School Students from the Perspective of Administrators, Teachers, and Students,” St. John Fisher University, Ralph C. Wilson, Jr. School of Education, Education Doctoral, https://fisherpub.sjf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1231&context=education_etd, retrieved July 2024.

7 Esther, H., 2015, “The Importance of Developing Leadership Skills in Grades 6–8 Middle School Students from the Perspective of Administrators, Teachers, and Students,” Fisher Digital Publications, https://fisherpub.sjf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1231&context=education_etd, retrieved July 29, 2024.

8 Esther, H., 2015, “The Importance of Developing Leadership Skills in Grades 6–8 Middle School Students from the Perspective of Administrators, Teachers, and Students,” Fisher Digital Publications, https://fisherpub.sjf.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1231&context=education_etd, retrieved July 29, 2024.

9 Montessori Flagstaff, 2024, “5 Interesting Ways Middle School Students Learn Leadership Skills,” Blog Post, www.flagmontessori.com/blog/5-interesting-ways-middle-school-students-learn-leadership-skills, additional material and content added by authors, retrieved July 9, 2024.

10 Kittelstad, K., n.d., “What’s the Difference between Ethics, Morals and Values?” https://Examples.yourdictionary.com/difference-between-ethics-morals-and-values.html, retrieved July 1, 2024.

11 The University of Texas at Austin, 2024, “Values,” Ethics Unwrapped – McCombs School of Business – The University of Texas at Austin, https://ethicsunwrapped.utexas.edu/glossary/values#:~:text=Values%20are%20individual%20beliefs%20that,values%20of%20their%20particular%20culture, retrieved August 7, 2024.

12 Amarillo College, 2023, “RSPT 1191 Introduction to Medical Ethics,” Amarillo College, https://ethicsunwrapped.utexas.edu/glossary/values#:~:text=Values%20are%20individual%20beliefs%20that,values%20of%20their%20particular%20cultur, retrieved August 7, 2024.

13 American Psychological Association (APA), November 15, 2023, “Dictionary of Psychology,” https://dictionary.apa.org/ethical-judgment, retrieved on August 7, 2024.

14 OpenAI, “Provide a Brief Definition of Norms as Used in the Field and Study of Ethics,” GPT-3.5, OpenAI’s large-scale language-generation model, https://chat.openai.com, chat.openai.com/c/6c151798-9d2d-482b-a075-db136c385112, prompt submitted November 18, 2023.

15 Marcella, A., May 21, 2024, Figure 1.2, "The Core Principles of Ethics," was designed and produced by the authors.

16 Monahan, K., 2012, "A Review of the Literature Concerning Ethical Leadership in Organizations," *Emerging Leadership Journeys*, 5(1). www.regent.edu/journal/emerging-leadership-journeys/ethical-leadership-definition-by-authors, retrieved August 5, 2024.

17 Barnes, C., & Doty, J. 2010, "What Is Ethical Leadership?", The Army Ethic 2010, MILITARYREVIEW,ArmyUniversityPress,UnitedStatesDepartmentoftheArmy,www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20100930ER_art015.pdf, retrieved August 2, 2024.

18 Lo Iacono, V., June 24, 2024, "Ethical Leadership: A Cornerstone of Success in Business and Effective Managerial Training, Eight Traits of Ethical Leadership," graphic reprinted and used with permission, Figure 1.3, https://symondsresearch.com/ethical-leadership/, retrieved August 5, 2024.

19 Mayer, B., February 12, 2024, "Why Generation Alpha Is Being Compared to Honey Badgers," Is Gen Alpha Really the Honey Badger Generation? (parents.com), retrieved August 14, 2024.

20 (n.a.), "Generation Alpha: The New Kids of America," Generation Alpha: the new kids of America (gwi.com), retrieved August 15, 2024.

21 The Anti-Bullying Alliance. https://anti-bullyingalliance.org.uk/aba-our-work, retrieved August 18, 2024.

22 U.S. Government Accounting Office (GAO), November 24, 2001, GAO analysis of the Department of Education's School Survey on Crime and Safety for school years 2015–2016 and 2017–2018, GAO-22-104341 as found in "K—12 Education: Students' Experiences with Bullying, Hate Speech, Hate Crimes, and Victimization in Schools, GAO-22-104341, Figure 1.4, www.gao.gov/products/gao-22-104341, retrieved May 25, 2024.

23 StopBullying.gov. www.stopbullying.gov/resources/laws, retrieved August 18, 2024.

24 Hate Generated Bullying, Figure 1.5, created by the Authors, May 9, 2024.

25 Crawford, M., June 2024, "How to Support Co-Workers Through Trauma," How to Support Co-Workers Through Trauma (alanet.org), retrieved August 22, 2024.

26 (n.a.), September 1, 2023, Newport Academy, "Signs that your Teen is being Bullied," Signs That Your Teen Is Being Bullied | Newport Academy, retrieved August 15, 2024.

27 University of the People. "Definition of Bullying," www.uopeople.edu/blog/definition-of-bullying/, retrieved August 18, 2024.

28 Preventing and Promoting Relationships & Eliminating Violence Network. "Types of Bullying," www.prevnet.ca/bullying/types, retrieved August 18, 2024.

29 The National Institutes of Health (NIH), 2024, "The Adolescent Brain Cognitive Development (ABCD) Study^{SM}," U.S. Department of Health & Human Services (HHS), https://abcdstudy.org/wp-content/uploads/2023/02/Screen-Time-ENGLISH.pdf, Figure 1.6, retrieved September 16, 2024.

30 Helmore, E, August 24, 2024, "Backlash Erupts Over Criticism of Tim Walz's Emotional Son: 'Families Are Everything'," www.theguardian.com/us-news/article/2024/aug/24/democratic-convention-tim-walz-son-emotions-criticized-backlash, retrieved September 16, 2024.

31 (n.a.), (n.d.) "Fast Facts: Preventing Bullying," The Centers for Disease Control and Prevention, About Bullying | Youth Violence Prevention | CDC, retrieved August 18, 2024.

32 U.S. Government Accountability Office, November 24, 2021, "K—12 Education: Students' Experiences with Bullying, Hate Speech, Hate Crimes, and Victimization in Schools," U.S. GAO, retrieved May 5, 2024.

33 (n.a.), (n.d.), International day against violence and bullying at school including cyberbullying | UNESCO, retrieved August 18, 2024.

34 StopBullying.gov, date last reviewed: October 6, 2021. "Federal Laws." www.stopbullying.gov/resources/laws/federal, retrieved February 8, 2024.

35 StopBullying.gov, date last reviewed: August 18, 2023. “Laws and Policies.” www.stopbullying.gov/resources/laws, retrieved August 18, 2024.

36 Yarborough, B., March 24, 2022, “Cyberbullying Victims are More Likely to Suffer from Depression. Here’s How to Spot it and Stop It,” San Bernardino Sun (sbsun.com), retrieved August 18, 2024.

37 Shutterstock, September 9, 2024, Figure 1.7, “Teasing Word,” Stock Vector ID: 2495916625, used under CRC License.

38 Lee, A. M. I., “The Difference between Teasing and Bullying,” www.understood.org/en/articles/difference-between-teasing-and-bullying, retrieved August 18, 2024.

39 Shutterstock, August 15, 2024, Figure 1.8 “Stop Bullying,” Stock Vector ID: 192355658, used under CRC License.

40 Meehan, Z. M., Hubbard, J. A., Moore, C. C., & Mlawer, F., 2024, “Susceptibility to Peer Influence in Adolescents: Associations between Psychophysiology and Behavior. Development and Psychopathology,” *Cambridge Core*, 36(1), 69–81. https://doi.org/10.1017/S0954579422000967, retrieved August 18, 2024.

41 Laursen, B., PhD, Episode 2, “Speaking of Psychology: The Good and Bad of Peer Pressure, with Brett Laursen, PhD,” American Psychological Association (apa.org), retrieved August 16, 2024.

42 Johnson, N., & Stixrud, W., August 18, 2022, “Helping Kids Become Good Decision Makers,” *Psychology Today*, www.psychologytoday.com/us/blog/the-self-driven-child/202208/helping-kids-become-good-decision-makers, retrieved August 18. 2024.

43 Viejo, C., & Toledano Fernández, N., October 30, 2021, “Teenage Brains: What Is Happening and Why It Leads to More Risky Behaviors”, *Neuroscience News*, retrieved May 7, 2024.

44 (n.a.) September 2017, American Academy of Adolescent and Child Psychiatry, “Teen Brain: Behavior, Problem Solving, and Decision Making” (aacap.org), retrieved May 7, 2024.

45 (n.a.), “Child’s Play: Kids as Young as Six Consider Choices in Moral Judgments”, *Neuroscience News*, https://neurosciencenews.com/moral-judgment-child-23350, retrieved June 5, 2024.

46 (n.a.), July 5, 2022, “Understanding Generation Alpha Characteristics,” Understanding Generation Alpha Characteristics – How They Are (studentcenteredworld.com), retrieved August 22, 2024.

47 (n.a.), (n.d.), MBA Research, About Us | Resources for Business Educators | MBA Research, retrieved June 5, 2024.

48 Betkowski, A., August 01, 2023, “Teaching Tuesday: What Is Character Education?” Teaching & School Administration, Grand Canyon University, www.gcu.edu/blog/teaching-school-administration/what-character-education#:~:text=Character%20education%20aims%20to%20develop,a%20world%20worth%20living%20in, retrieved August 18, 2024.

49 MBA Research, 2016, Figure 1.9, “Daniels Fund Ethics Initiative,” MBA Research, reprinted with permission, www.mbaresearch.org/about-us/daniels-fund-ethics-initiative, retrieved June 5, 2024.

50 Salek, E., October 4, 2022, “Making Important Decisions Together”, Center for Parent and Teen Communication, Making Important Decisions Together (parentandteen.com), retrieved August 18, 2024.

51 Watson, N., 2024, *Taming the Machine: Ethically Harness the Power of AI*. London: Kogan Page Publisher, p. 83. ISBN 978-1398614321.

52 Fortune, August 5, 2024, “Artificial Intelligence Market,” Fortune Business Insights, www.fortunebusinessinsights.com/industry-reports/artificial-intelligence-market-100114, retrieved August 19, 2024.

53 Marcella, A., August 10, 2024, Figure 1.10, "AI Usage in Education: 4 Tenets," was designed and produced by authors.

54 White, S., Scott, A., & Koshy, S., January 18, 2024, "Responsible AI & Tech Justice: A Guide for K—12 Education," Kapor Foundation, https://kaporfoundation.org/wp-content/uploads/2024/01/Responsible-AI-Guide-Kapor-Foundation.pdf, used with permission as provided through CC BY-ND 4.0, Attribution-NoDerivatives 4.0 International, Creative Commons License, http://creativecommons.org/licenses/by-nd/4.0/, retrieved August 20, 2024.

55 Marcella, A., & Renz, G., January 2024, "Generative Artificial Intelligence: Benefits and Risks to Law Firms," Association of Legal Administrators, www.alanet.org/publications/white-papers/generative-artificial-intelligence-benefits-and-risks-to-law-firm.

56 Marcella, A., May 17, 2024, "The relationship between AI, NLP, ML, DL, and ANNs," Figure 1.11, drawn by the authors.

57 Cotton, P., Patel, M., & Wei, W., May 2022, "The Foundational Standards for AI ISO/IEC 22989 and ISO/IEC 23053," ISO/IEC AI Workshop, chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://jtc1info.org/wp-content/uploads/2022/06/03_08_Paul_Milan_Wei_The-foundational-standards-for-AI-20220525-ww-mp.pdf, Figure 1.12 redrawn by authors, retrieved February 11, 2024.

58 Shutterstock, 2024, Figure 1.13, "Training AI," Shutterstock image, Stock Photo ID: 2429626257, used under CRC License, August 10, 2024.

59 White, S., Scott, A., & Koshy, S., January 18, 2024, "Responsible AI & Tech Justice: A Guide for K—12 Education," Kapor Foundation, https://kaporfoundation.org/wp-content/uploads/2024/01/Responsible-AI-Guide-Kapor-Foundation.pdf, retrieved August 19, 2024.

60 Google Cloud, n.d., "What are AI hallucinations?" https://cloud.google.com/discover/what-are-ai-hallucinations#:~:text=started%20for%20free-,How%20do%20AI%20hallucinations%20occur%3F,making%20incorrect%20predictions%2C%20or%20hallucinating, retrieved August 10, 2024.

61 Barney, N., March 2023, "deepfake AI (deep fake)," TechTarget, www.techtarget.com/whatis/definition/deepfake, retrieved February 10, 2024.

62 Paresh, D., July 31, 2024, "Google Cracks Down on Explicit Deepfakes," Wired, www.wired.com/story/google-tries-to-crack-down-on-explicit-deepfakes/, retrieved August 11, 2024.

63 Marcella, A., 2024, Figure 1.14, "Risks of Unethical AI," graphic drawn by authors.

64 Marcella, A., 2024, Figure 1.15, "Benefits of Ethical AI Use," graphic drawn by authors.

65 Grace, K., Stein-Perlman, Z., Weinstein-Raun, B., & Salvatier, J., August 3, 2022, "2022 Expert Survey on Progress in AI." AI Impacts. https://aiimpacts.org/2022-expert-survey-on-progress-in-ai/, retrieved August 11, 2024.

66 Figure 1.16, redrawn by authors, from Katja Grace, Zach Stein-Perlman, Benjamin Weinstein-Raun, and John Salvatier, "2022 Expert Survey on Progress in AI." AI Impacts, August 3, 2022. https://aiimpacts.org/2022-expert-survey-on-progress-in-ai/, retrieved August 11, 2024.

67 Crabtree, M., August 2923, "What is AI Literacy? A Comprehensive Guide for Beginners," www.datacamp.com/blog/what-is-ai-literacy-a-comprehensive-guide-for-beginners, retrieved August 19, 2024.

68 Perez, S., November 16, 2023, "Several Popular AI Products Flagged as Unsafe for Kids by Common Sense Media," https://techcrunch.com/2023/11/16/several-popular-ai-products-flagged-as-unsafe-for-kids-by-common-sense-media, retrieved August 19, 2024.

69 Marcella, A., August 2024, Figure 1.17, "Basic Components of genAI Literacy," drawn by authors, produced on August 17, 2024.

70 Ng, D. T. K., Leung, J. K. L., Su, J, Ng, R. C. W., et al., 2023, "Teachers' AI Digital Competencies and Twenty-First Century Skills in the Post-Pandemic World," *Educational Technology Research and Development*, 71(1), 137–161. https://doi.org/10.1007/s11423-023-10203-6. Epub 2023 Feb 21. PMID: 36844361, PMCID: PMC9943036, retrieved May 26, 2024.

2

TECHNOLOGY AND CYBER SAFETY

Teaching Tomorrow's Digital Citizens

Introduction

The Internet allows access to information 24 hours a day, 7 days a week, 365 days a year. For schools (public and nonpublic), online capabilities can provide access to resources that facilitate remote learning in an online setting and collaboration between classes and students in different locations.

However, the Internet can also serve as a channel for threats that negatively impact the whole school community. Students are at risk from online threats like sextortion and cyberbullying. Threats in an online environment can have serious impacts; for example, cyberbullying can lead to depression and anxiety, health complaints, and decreased academic achievement by students.[1]

This chapter examines issues of our digital world, including emerging technologies that present exposures, high risks, and challenges for seventh- and eighth-grade students. While these issues are universally present and will affect everyone differently, students at this grade level are gaining more online independence and being exposed to more cyber influence than in previous grades. These issues can present challenges and risks that are physical, and emotional and may have varying long-term effects on students.

Incorporating discussions and designing assignments addressing these issues will reinforce to students the importance of remaining cyber-safe online and offline.

Transitioning from Monitoring to Teaching

This chapter examines a breadth of topics, each an essential learning opportunity for students.

Educators and parents acknowledge that as students mature and move from children in the earliest academic grades to young adults (tweens and teenagers) in the seventh and eighth grades, transitioning from monitoring student online behavior to teaching students and equipping them with the skills necessary to identify cyber risks is vitally important.

This essential cyber-aware, cyber-safe skill set will empower students to become independently proactive in establishing and sustaining a personal cyber safety outlook that is essential in today's digitally dominated and dependent world.

DOI: 10.1201/9781003466376-2

Cyber Smart: Empowering Student Digital Citizens

The following issues raise a cause for concern and represent a risk to students. Educators, by addressing these issues with their students, will empower each student to take personal responsibility for his or her cyber safety.

Educators should consider discussing and incorporating into in-class and out-of-class exercises and assignments the following critical issues that directly affect and impact a student's mental health and cyber safety in our evolving digital society…

- Online Privacy and Personal Data Protection
- Cyberbullying Awareness and Prevention
- Social Media and Networking Practices
- Password Security and Account Protection
- Recognizing and Avoiding Phishing Scams
- Understanding Digital Footprints
- Fake News and Media/Information Literacy
- The Impact of Screen Time
- Ethical Use of Technology
- Risks of Digital Social Networking (DSN): Inappropriate Content
- Digital Literacy
- Basic Cybersecurity Awareness

It is important to recognize that the above list is not complete, nor will it ever be. The issues identified reflect the current status of our digital world. As this digital environment grows, changes, and is directly affected by new and emerging technologies, students will face, new risks, new challenges … new issues, as they continue to live, grow, and work in a digital society.

Online Privacy and Personal Data Protection

This topic covers the importance of protecting personal information online, understanding privacy settings on social media, and recognizing the risks of sharing too much information.

Teaching students about online privacy is crucial, as they are increasingly using digital platforms. Understanding how to manage personal data helps to mitigate identity theft, cyberbullying, and unauthorized access to personal information (theirs as well as family members and friends). Continued discussion and tailored exercises on taking steps to proactively protect their privacy fosters responsible digital habits and empowers students to take control of their online presence.

Oversharing

Sharing information online can be risky. Oversharing can occur via private channels, like instant messaging, or through public channels, such as social media posts, online chat rooms, or other public online forums.

Personal information as well as personally identifiable information (PII) may be shared online by students or other school community members. This information might include name, age, address, phone number, passwords, Social Security number, and family financial information (including credit card numbers or bank account details). PII and other student and staff information are valuable to malicious cyber actors, as this information can be used to commit identity theft, sold to other threat actors,[I] and used to develop and carry out other cyberattacks.

Students are also at risk of online child sexual exploitation and abuse. Sharing sexually explicit images or videos, even with individuals believed to be known and trusted, can lead to other serious online threats, including sextortion.

Oversharing may also have academic or professional consequences for a student or staff member. It is important to think carefully before posting images or language online, on social media, or other shared messaging platforms.

It is important to discuss with students the "permanence of the Internet," meaning that whatever they post will have a very long shelf-life, and in most cases, reach a permanent existence in a multitude of virtual, publicly accessible files and libraries. This means that future employers, coaches, college admissions officers, law enforcement professionals, and others may all be able to see what a student posts and shares online.

Many posts may have been written (or images taken) when the student was younger; however, later in life, such posts and images may be viewed as offensive and ultimately prove damaging to the student's adult life and career.

Recommendations — Achieving Online Privacy and Personal Data Protection

The following are recommendations to discuss with your students for achieving online privacy and personal data protection.

Think Before You Post Remind students that what they post online may remain there for a very long time. That meme might be funny now, but in the future, students may not want these posts publicly available to anyone who goes searching (e.g., employers, law enforcement, political rivals, future spouse(s), etc.).

It is important to note that data lives as long as its storage media. Just as paper fades and disintegrates over time, so does most — if not all — digital media, as it exists today. As data storage media become more sophisticated, the shelf-life longevity of data's lifespan will increase.

Given the reality of the above statement, it is still prudent for students to think twice (sometimes more) before clicking "send." That email, meme, TikTok video, etc., may be around long enough for someone to find it and to cost the student a job, a loan, or a friend.

[I] A "threat actor" is a person or group responsible for carrying out actions that can harm or disrupt a computer system (personal/individual or enterprise/business), network, or organization. They can be hackers, cybercriminals, or even insiders with malicious intent. Their goal is often to steal data, cause damage, or exploit security weaknesses.

Check Privacy Settings Advise students to always set their social media accounts to private.

Remind students that whatever they post on social media, even when that information is set for private audiences, could someday become public due to data breaches, poor data management practices, or data brokering. Inform them that in some cases, a site's terms of service explicitly claim ownership of all posted content (this can include posted photos and or music created by the student).

Advise students to enable strict privacy settings that block data sharing between apps. For even more control over their privacy, students should opt out of saving login passwords within application settings and disable all error/debug reports. Have students review privacy settings quarterly. Failure to set security measures can provide threat actors with unauthorized access to their data.

Tell them that setting their social media accounts to private is like having a guest list for a birthday party — they wouldn't let anyone walk in, so don't let anyone access their online profiles, email accounts, photos, phonebooks, etc.

Use Secure Apps and Websites This one should be well known by your students, but it is worth repeating and reviewing. Remind students to only download apps and visit safe and secure websites. For example, before downloading a new game, check reviews and ratings to make sure it's legit, just like you'd ask friends for a movie recommendation.

How Can You Tell If a Website Is Legitimate? Listed below are ten ways to check if a website is legitimate, along with examples to help your students understand how to apply each method:

- Check for HTTPS Security: Ensure the URL starts with "https://" and look for a padlock icon. For example, when students visit their online banking site, the URL for the bank's website should begin with "https://" and show a padlock symbol indicating it's encrypted.
- Look at the URL Carefully: Alert students to be cautious of URLs with misspellings, extra characters, or strange domain names. Instead of "www.amazon.com," a scam site might use www.amaz0n.net — a subtle but important difference.
- Check the Domain Age: Guide students in the use of tools like WHOIS[II] to check how long a website has been active. Legitimate sites are usually older. Scammers might create a site that's only been live for a few days or weeks to trick people during the holidays.

[II] Every domain name that's been registered belongs to someone, and by default, that registration information is public. WHOIS [www.domain.com/whois/whois] is a way of storing that information and making it available for the public to search.

- Verify the Domain: Subtle changes are hard to notice, such as a zero instead of a capital letter "O." Some are harder to spot, but one indicator of an illegitimate site could be multiple "word.com" sequences in the URL.

  There should be only one domain in the web address. You might see something you recognize, like "chase.com." However, there shouldn't be more than one ".com," ".org," ".net," etc. For example, a Chase website wouldn't be "chase.com/bank/account.chase.org." The last domain in the address (chase.org) is incorrect.[2]
- Verify Contact Information: A legitimate website will provide real contact details, including an email, phone number, and physical address. Check if an online store lists a customer service phone number that works, and search for the business address on Google Maps.
- Read the Website's Privacy Policy: Legitimate websites have clear privacy policies explaining how they handle your data. Look at a website's footer for links to a privacy policy before submitting personal information.
- Check for Trust Seals: Look for trusted security seals from security organizations such as… Norton, McAfee, or the Better Business Bureau, but verify that they're clickable and link to official verification pages. For example, if a McAfee seal is present, click on it to make sure it's authentic and leads to the official McAfee website.
- Look for Grammatical Errors: Fake websites often contain spelling or grammar mistakes, especially in important sections like product descriptions or legal information. Have students examine a website's "About Us" link. In doing so, if they were to find multiple errors in the "About Us" section, that might be a red flag that the site isn't professional or legitimate.
- Research Reviews and Reputation: Have students practice searching for reviews of the website on independent platforms like Trustpilot or Google Reviews. Generally, if an online store has no reviews or only overly positive ones, students should be advised to view these sites as suspicious and with caution.
- Check for Safe Payment Options: A legitimate site will use secure payment methods like credit cards or PayPal. Avoid sites that only ask for wire transfers or gift cards. Warn students that if a shopping website only asks for payment via gift cards, it's likely a scam.
- Test the Website's Social Media Presence: Instruct students to check if the website has active and legitimate social media accounts. Scam websites usually have no social media presence or fake profiles. A legitimate business will likely have an Instagram or Facebook page with real interactions, not just stock photos and fake comments.

Beware of Public Wi-Fi Discuss with students the importance of not logging into important accounts on public Wi-Fi. While the temptation is there, it will only be a minute to check an account balance or to order an item while grabbing a quick bite or refreshment at a local restaurant.

Remind students that logging into their social media account(s), their bank account, or online shopping account on public Wi-Fi is like writing their account password/passphrase and posting it to their Facebook account or on X or TikTok, for anyone to see. Don't use unsecured, public Wi-Fi.

Maintaining Online Privacy and Protecting Personal Data: A Student Quiz

The North Carolina Department of Information Technology (NCDIT) offers a set of questions that students should ask themselves to assess if they are keeping their personal information safe.

Teaching Tip

Educators may wish to review these questions with students in a classroom setting or with student groups selecting and discussing specific questions and reporting back to the entire class.

Students should ask themselves:

- Am I posting sensitive information? This means addresses, phone numbers, your birthdate, Social Security number, driver's license number, or financial information.
- Should I share this? Be careful posting details about your life, and don't answer questions — online or over the phone — from anyone you don't know asking personal questions.
- What are the privacy settings on my accounts? Look through the settings of the social media you use to be sure only people you absolutely trust see your posts.
- Should I click? Unexpected links and attachments in messages might contain viruses or spyware that the sender doesn't even know about. Check with the sender first. If you don't know the sender, just trash the message.
- Is this site legitimate? Malicious websites can look identical to trusted sites, but the URL or email address might use a different spelling or domain (e.g., net instead of.com). When in doubt, avoid the website until you're 100% sure.
- Is my software up to date? Check to be sure you're running the latest operating system (OS), antivirus software, and web browsers.
- Is it too good to be true? Free games and other things might be tempting, but they can come at a cost to your privacy. Only download from trusted sources, even if you might have to pay.
- Are my passwords safe? Be sure your passwords include a mix of upper and lowercase letters, numbers, and symbols. Make them hard enough that someone can't guess them, and don't share them with anyone. Better yet, use passphrases!
- Am I using free Wi-Fi? Many public Wi-Fi hotspots — like libraries and coffee shops — aren't secure and might not protect your passwords, messages, photos, and other data. Check with an employee before connecting.[3]

Maintaining an ongoing dialogue with students about the necessity of being diligent in establishing cyber-safe habits through in and out-of-class assignments will better prepare students to take responsibility and control their online privacy and personal data protection requirements.

Cyberbullying Awareness and Prevention

Cyberbullying involves using digital devices like cell phones, computers, and tablets to harass, threaten, or embarrass others. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming, where people can view, participate in, or share content.

Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else, causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behavior.[4]

With the rise of social media and online communication, cyberbullying has become a significant issue. Discussing this with students helps them recognize harmful behaviors, know how to respond, and understand the emotional impact on victims. Early intervention can prevent long-term psychological effects and promote a safer online environment.

The reader is directed to Chapter 3, where this topic and the role that cyberbullying plays in affecting both student mental health and cyber safety have been addressed extensively.

Social Media and Networking Practices

> Up to 95% of youth ages 13–17 report using a social media platform, with more than a third saying they use social media "almost constantly." Although age 13 is commonly the required minimum age used by social media platforms in the U.S., nearly 40% of children ages 8–12 use social media.[5]
>
> — *The U.S. Surgeon General*

Social Media or Social Networking?

Social media refers to the platforms where people create, share, and consume content such as videos, photos, blogs, and posts. It's primarily about broadcasting information. Social networking refers to the act of connecting with others and building relationships through communication and interaction on these platforms. It's about engaging directly with people.

In general, people often use the terms social media and social networking interchangeably, although they have distinct meanings.

Table 2.1 Social Media vs. Social Networking

SOCIAL MEDIA EXAMPLE	SOCIAL NETWORKING EXAMPLE
YouTube: Sharing and watching videos with limited interaction (likes and comments).	**Facebook groups**: Joining groups to engage in ongoing discussions and building relationships.
Instagram posts: Posting images or stories for followers to like and comment on.	**Discord servers**: Participating in real-time chats, creating communities, and building connections through conversations.
TikTok: Posting short, entertaining videos that others can watch and react to.	**LinkedIn**: Connecting with professionals to exchange messages, build networks, and discuss career-related topics.
Snapchat stories: Sharing temporary photos or videos with minimal interaction.	**X (formally Twitter) threads**: Engaging in extended conversations or debates, fostering discussions and connections.
Pinterest: Saving and sharing images or ideas, with minimal interaction from others.	**Reddit**: Joining topic-specific communities to post, comment, and engage in discussions with others.

This can certainly confuse users because many platforms offer both functionalities. Facebook users, for example, can share posts (which is a social media aspect) while also joining groups and interacting directly with others (which is a social networking aspect). Similarly, X (formerly Twitter) allows users to post thoughts or links (social media) but also engage in conversations (social networking). This blending of services promotes the generally accepted interchangeable use of the terms, even though they refer to different types of online activity.

The definition of social media has been highly debated over the past few decades. As a result, there isn't a single, widely accepted scholarly definition of social media.[6]

Our digital society today does not distinguish between the two, and they are often discussed together under the broad term "social media." However, understanding the difference is essential, particularly when analyzing how individuals use these platforms, either for content consumption or relationship building.

Table 2.1 provides comparative examples of social media and social networking.

Social Media

Social Media: Is It Safe Out There?

Safe social media practices address how students can use social media responsibly, including understanding the implications of their online actions, the permanence of digital footprints, and managing online interactions.

Nearly every teenager in America uses social media, and yet we do not have enough evidence to conclude that it is sufficiently safe for them.

A longitudinal cohort study of US adolescents aged 12–15 ($n=6{,}595$) found that adolescents who spend more than 3 hours per day using social media may be at heightened risk for mental health problems, particularly internalizing problems. Poor emotion regulation and lack of social interaction may also be associated with social media use and contribute to symptoms of anxiety and depression.[7]

Social media is a primary communication tool for many young people. Educating students on safe practices helps them avoid risks like online predators, inappropriate content, and reputational damage. Understanding the long-term consequences of their online behavior is essential for developing responsible digital citizens.

Social media use by youth is nearly universal. Up to 95% of youth ages 13–17 report using a social media platform, with more than a third saying they use social media "almost constantly." Although age 13 is commonly the required minimum age used by social media platforms in the United States, nearly 40% of children ages 8–12 use social media. There are increasing concerns among researchers, parents and caregivers, young people, healthcare experts, and others about the impact of social media on youth mental health.[8]

Social media can provide benefits for some youth by providing a positive community and connection with others who share identities, abilities, and interests. It can provide access to important information and create a space for self-expression, identity development, aspirational development, and peer engagement.[9]

The use of social media during adolescence can also negatively impact health and development.

A study conducted among 14-year-olds ($n = 10{,}904$) found that greater social media use predicted poor sleep, online harassment, poor body image, low self-esteem, and higher depressive symptom scores with a larger association for girls than boys.

A majority of parents of adolescents say they are somewhat, very, or extremely worried that their child's use of social media could lead to problems with anxiety or depression (53%), lower self-esteem (54%), being harassed or bullied by others (54%), feeling pressured to act a certain way (59%), and exposure to explicit content (71%).[10]

Healthy vs. Unhealthy Social Media

Healthy social media is characterized by balanced, positive interactions, self-awareness, educational content, and mindful usage. In contrast, unhealthy social media often involves harmful behavior like cyberbullying, misinformation, addiction, and negative emotional impacts due to comparison or overexposure.

Table 2.2 provides examples of the differences between healthy and unhealthy social media.

Social Media's Impact — Good and Not-so-Good

Social media can provide many benefits to students, ranging from educational assistance (e.g., tutorials, informative videos, and discussions on various topics), to engagement with peers (e.g., staying connected with friends and classmates outside of school for group projects, study groups, or just maintaining friendships), and furthering skill

Table 2.2 Healthy Social Media vs. Unhealthy Social Networking

HEALTHY SOCIAL MEDIA TRAITS/ACTIVITIES	UNHEALTHY SOCIAL MEDIA TRAITS/ACTIVITIES
Positive interactions: Engaging in supportive and constructive conversations with others, promoting kindness and understanding.	**Cyberbullying or harassment**: Using platforms to harm, bully, or target individuals through negative comments or messages.
Educational content: Following and sharing posts that inspire learning or personal growth, such as tutorials, informative articles, or positive news.	**Misinformation**: Sharing or spreading false or misleading information without fact-checking, which can harm individuals or communities.
Mindful usage: Setting limits on screen time and ensuring a balance between online and offline activities to avoid excessive use.	**Excessive usage**: Spending too much time on social media, leads to potential issues like reduced productivity, poor mental health, or disrupted sleep patterns.
Authenticity: Posting content that reflects true experiences and emotions, fostering genuine connections with others.	**Comparing and competing:** Constantly comparing oneself to unrealistic portrayals of others' lives, can lead to anxiety, low self-esteem, or depression.
Privacy awareness: Understanding and controlling privacy settings to protect personal data and being cautious about sharing sensitive information.	**Over-sharing personal details**: Sharing private or sensitive information publicly, making one vulnerable to identity theft or privacy breaches.

development (e.g., platforms like Instagram and TikTok) can encourage creativity through video editing, photography, and content creation, helping students develop digital literacy skills, which are essential in today's digitally dependent, digitally driven world.

According to the 2023 "Children and Parents: Media Use and Attitudes" report, released by the UK Office of Communications (Ofcom), parents and children identified positive benefits of being online, especially concerning learning (81% of children, 84% of parents) and to building and maintaining friendships (68% of children, 65% of parents).[11]

Social media provides students with additional benefits such as access to global communities, a platform to express themselves through posts, videos, and art, developing critical thinking, and career awareness.

The potential risks of social media may be especially acute, however, during early adolescence when puberty delivers an onslaught of biological, psychological, and social changes. One longitudinal analysis of data from youth in the United Kingdom found distinct developmental windows during which adolescents are especially sensitive to social media's impact. During those windows, around 11–13 for girls and 14–15 for boys, more social media use predicts a decrease in life satisfaction a year later, while lower use predicts greater life satisfaction.[12]

A study of 2,000 Gen Z social media users commissioned by LG Electronics and conducted by Talker Research, revealed…

- Three in four Gen Zers are blaming social media for having a negative impact on their mental health.
- Gen Z Americans who use social media, found Instagram (20%), TikTok (20%), and Facebook (13%) have all had a negative impact on their well-being.

- Social media scrolling leaves nearly half of Gen Zers (49%) feeling some kind of negative emotion, like stress and anxiety (30%).
- Those who experience negative emotions report that it only takes them 38 minutes on social media before they start to feel bad.
- Respondents attribute these feelings to consuming upsetting content (51%), feeling unproductive with how they spent their time (49%), and/or experiencing fear of missing out (FOMO) (36%).
- 62% of Gen Zers responding to the survey wish they could "reset" their social media feeds and start over again.
- Two-thirds (65%) have turned a bad day into a good one because of what they've seen on social media. Adding to this, respondents were 70% more likely to use social media when they are in a good mood compared to a bad mood, and 44% believe social media has a positive impact on their outlook on life.[13]

Do You Know Kik?

Well, as of 2024 over 300 million people do and 70% of Kik users are aged between 13 and 24 years old! There is a very high probability that your students know about and use Kik.

One of the primary reasons for Kik's widespread popularity is its minimal sign-up requirement — users *only need an email address. No additional identification is necessary*, which significantly simplifies the registration process and encourages easy participation. It also makes it very easy for ANYONE, regardless of age to sign up for a Kik account. Be that individual a 13-year-old or a 45-year-old pretending to be a 13-year-old!

One of Kik's most appealing features is that users can engage in conversations with complete strangers. No questions asked, none … except what group do you wish to join? Who do you want to meet? Users can immediately message anyone they meet — privately, with both sides to the conversation remaining completely anonymous.

Table 2.3 identifies the top risks associated with the Kik app. These risk concerns should be discussed with young adults and really with any individual (at any age under 18) having access to social networking sites in general, be they supervised or not.

Educators (parents, caregivers), be prepared to discuss this social networking app with your students (children), advising them of the risks associated with the app and providing PII to anyone without first confirming who that individual is.

Safer Social Media for Students: Recommendations

Given the proof that social media can be both harmful as well as beneficial, educators may use the following list of recommendations as teaching and learning aids or

Table 2.3 Risks Associated with the Kik App

RISK		REASON FOR CONCERN
Anonymity and lack of age verification	Kik allows users to sign up with just an email, without verifying their age or identity. This opens the door for minors to misrepresent their age, and it allows adults or malicious individuals to create anonymous profiles and contact children.	Educators and parents should be worried about the potential for predatory behavior, as adults can easily pose as children and attempt to exploit or manipulate younger users.
Inappropriate content	Kik has a reputation for allowing the sharing of explicit and inappropriate content. Users can exchange images, videos, and messages that may be unsuitable for children.	Exposure to explicit content can have a lasting impact on a child's development, desensitizing them to sexual and violent materials and contributing to potential trauma or unhealthy views of relationships and boundaries.
Private and unmonitored chats	Kik features private one-on-one and group chats, where conversations are not monitored or filtered. Users can communicate freely with strangers, creating a space for cyberbullying, sexting, or harmful peer pressure.	Parents and educators may have limited or no visibility into these conversations, increasing the risk of harmful interactions and the potential for children to be targeted by bullies, predators, or to engage in risky behavior.
Cyberbullying	Due to the anonymous and unmonitored nature of the platform, Kik can become a breeding ground for cyberbullying, where students can be harassed, humiliated, or threatened by peers or strangers.	Cyberbullying has severe consequences, including emotional distress, anxiety, depression, and in some cases, self-harm. Middle school children, who are particularly vulnerable to social pressure, may struggle to cope with online bullying.
Third-party bots and external links	Kik allows integration with third-party bots, games, and external links, which can expose children to malicious content, phishing, scams, or attempts to steal personal information.	Children may be unaware of the dangers of interacting with these bots or clicking on external links, which can compromise their personal information, lead to financial scams, or expose them to harmful websites.

tips to discuss with and present to their students as ways students can better protect themselves and make their social media experiences safer.

Have an open discussion with students on social media cyber-safe practices and cover these important points…

- Identify Critical Information: Critical information is any information considered sensitive or that could harm (the owner, i.e., student or the student's family, friends, etc.) if compromised. What critical/sensitive information is on your mobile devices, online accounts, etc., that does not need to be there? If it is not essential, delete it.
- Update Immediately and Frequently Review Privacy Settings: Adversaries prefer easy targets. Direct students to ensure that their computing devices, software, and applications are updated as soon as patches are available. Instruct students to review previous privacy settings after each update to ensure they have not been reset.
- Protect Your Location Data: Pictures posted on social media may be recognizable or have additional data stored in metadata, which may expose a

person's location. To mitigate this, students should disable location services settings on the device/application and not voluntarily give their location away by using social media platforms to geo-tag or "check-in" at various public locations. Additionally, apps should be given as few permissions as possible, especially social media apps.

Teaching Tip

Have students investigate the apps listed in Table 2.4 to see how technology (including AI) is employed to identify location information from photos, reinforcing the need to protect their location data.

- Stress to students that they MUST verify every friend request they receive to make sure it is actually the person they know. Let students know that they can always ask a trusted adult to call or meet the person face-to-face to confirm they sent the invite. Continue to advise students that they should never accept invites from people they don't know.

- Plain and simple … tell students not to post critical information. If they don't want that information publicly available, don't post it. Even if a student deletes a post or an image/meme, in reality, nothing deleted from the Internet is ever truly removed.
- Strongly advise students to refrain from filling out surveys asking personal questions for social media posts. These surveys often ask for personal

Table 2.4 Apps That Can Identify the Location of a Photo

APP NAME	DESCRIPTION	WEBSITE URL
GeoImgr	GeoImgr reads the EXIF metadata from a photo to reveal location details and allows users to edit the geotags or add new ones for SEO purposes.	www.geoimgr.com
GeoSetter	A Windows app that helps you view and edit location data from photo EXIF metadata information, using various map sources like Google Maps or OpenStreetMap.	www.geosetter.de
Google Lens	Google Lens can identify objects, landmarks, and locations in images using Google's extensive database, but it doesn't directly extract location metadata.	lens.google.com
Photo investigator	This app reveals detailed EXIF data, including location metadata, allowing users to investigate and modify photo information such as GPS coordinates.	apps.apple.com
Pic2Map	This tool extracts the EXIF metadata from an image, including GPS coordinates, and displays the location on a map. It also provides additional camera and photo data.	www.pic2map.com
Picarta.ai	Picarta uses AI to identify the location of a photo by analyzing image content. After uploading a photo, it provides detailed location data based on visual cues and landmarks.	www.picarta.ai
TinEye	TinEye is a reverse image search engine that helps identify where an image appears online but doesn't focus on geolocation or EXIF metadata extraction.	tineye.com

EXIF (Exchangeable Image File Format) metadata is a set of information automatically stored within an image file when a photo is taken. It includes details such as the camera settings (e.g., shutter speed, aperture, ISO), the date and time the photo was taken, and if available, GPS coordinates showing where the photo was captured. This metadata helps provide context for the image, allowing users or apps to retrieve technical and location-based details about the photo.

information, and this information may be used by threat actors to compromise accounts and reset passwords.

- Warn students not to post sensitive, privileged, private, or confidential data in their status messages or timelines. When selecting who can access their posts, pages, or profiles, limit access to friends only and avoid allowing full public access to any of their content. Malicious parties who gain access to these sensitive/private data/images/messages, etc., can also use this information to extort or blackmail them.
- Make sure to discuss with students the importance of being aware of their physical and virtual surroundings. Accessing social media applications from open Internet hotspots provided at cafés, restaurants, and even when traveling at airports may leave their mobile devices susceptible to threat actors who can physically and virtually spy on their online activities. Students should be taught to know, remember, and not forget … do not connect to networks if they're not familiar with them or can't verify their authenticity.
- Students should be made aware of how to recognize social engineering tactics. Advise students to be cautious of surveys, shared posts, or quizzes that ask for personal information that could lead to an answer to a security question. For example, a seemingly innocuous post may state: "What is your school's mascot? Help us identify the most popular school mascot. Tell us yours in the comments below!" A threat actor can use posts like this to collect answers for future malicious, unauthorized access attempts or to guess passwords. Remind students that if anyone is asking for personal information, be cautious and think about (a) why this person is asking me for this information, (b) who might use this information, and (c) for what purposes.

For parents and caregivers…

- Setting limits and boundaries around social media, combined with discussion and coaching from adults, is the best way to promote positive outcomes for youth. Educators (to their students) and parents (to their children) should talk often about social media, technology, and the risks. Parents should consider using strategies like limiting the amount of time teens can use devices and removing devices from the bedroom at night.[14]
- Caregivers should also keep an eye out for problematic behaviors, such as strong cravings to use social media, an inability to stop, and lying or sneaking around to use devices when they aren't allowed.
- Adults should monitor kids' social media use closely in early adolescence, between the ages of 10 and 14 or so. As kids become more mature and develop digital literacy skills, they can earn more autonomy.[15]
- Adolescents' social media use should be preceded by training in social media literacy to ensure that users have developed psychologically informed competencies and skills that will maximize the chances for balanced, safe, and meaningful social media use.[16]

Educators can share with students and incorporate into out-of-class assignments the US Department of Homeland Security's "Top 10 Tips2Protect for Teens" with students. These tips will assist students in strengthening their awareness of social media risks while increasing their overall cyber safety in the digital world in which they live, work, and play.

Teaching Tip

1. Set all apps, games, social media accounts, and devices to private.
2. Turn off location data services on social media and all apps, except the ones your family uses to keep track of where you are. Talk to a trusted adult about which apps need location services and which don't.
3. Remember, anything posted online can be found later, even if it's deleted. After it's sent, you can't take it back.
4. Don't believe that everyone is who they say they are online.
5. Know who is on your friend lists. Remove strangers. Only accept friends you know in real life.
6. Never leave a game to chat on a different platform with someone you don't know.
7. Don't respond to messages or requests from people you don't know.
8. If something happens that makes you feel uncomfortable or you feel like something's just not right, tell an adult you trust, such as a parent, relative, teacher, or family friend.
9. Do not delete messages or images. Save usernames, screenshots, and images as evidence.
10. Don't panic. You're not alone. There are many ways you can get help.[17]

Social Networking

DSN or simply social networking sites such as Facebook, X (formally Twitter), LinkedIn, WhatsApp, Instagram, and Pinterest, are attracting multitudes of users daily, with the most popular online services totaling over half a billion users.

Educators should discuss the risks of DSN with students because it provides them with the awareness and tools necessary to participate in today's online society safely.

Social networking platforms can expose students to privacy vulnerabilities, such as data breaches or the collection of personal information. Educators can teach students about securing their accounts, recognizing phishing attempts, and understanding the consequences of sharing too much information online, which can lead to identity theft, cyberbullying, or exposure to inappropriate content.

Discussing digital risks helps students understand the emotional and psychological impacts of social networking. Peer pressure, cyberbullying, and the potential for unhealthy comparisons on these platforms can negatively affect students' self-esteem and mental health. By fostering conversations about responsible online behavior and

Table 2.5 Ways for Students to Mitigate Social Networking Risks

Reach out for help.	• If you or someone you know is being negatively affected by social media, reach out to a trusted friend or adult for help.
Create boundaries to help balance online and offline activities.	• Limit the use of phones, tablets, and computers for at least 1 hour before bedtime and through the night to enable sufficient and quality sleep. • Keep mealtimes and in-person gatherings device-free to help build social bonds and engage in two-way conversations with others. • Nurture your in-person relationships by connecting with others and making unplugged interactions a daily priority.
Develop protective strategies and healthy practices	• Track the amount of time you spend online. • Block unwanted contacts and content. • Learn about and use available privacy and safety settings. • Learn and utilize digital media literacy skills to help tell the difference between fact and opinion. • Ensure you are connecting with peers in-person.
Be cautious about what you share.	• Personal information about you has value. • Be selective with what you post and share online and with whom, as it is often public and can be stored permanently. • If you aren't sure if you should post something, it's usually best if you don't.
Protect yourself and others.	Harassment that happens in email, text messaging, direct messaging, online games, or on social media is harmful and can be cyberbullying. • Don't keep online harassment or abuse a secret. • Don't take part in online harassment or abuse.

The U.S. Surgeon General, 2023, "Social Media and Youth Mental Health," The U.S. Surgeon General's Advisory, www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf, retrieved September 9, 2024.

the importance of digital footprints, educators help students develop critical thinking skills about their social interactions online, empowering them to make safer, more informed choices, and become more dynamic digital citizens.

Be Self-Aware: Mitigate Potential Social Networking Risks

Discussions with students may include recommending ways that students should take to mitigate the potential risks of social networking and use social media safely and healthily.

Recommendations to discuss with students to accomplish this objective can be found in Table 2.5.

Parental Controls and Open Dialogue: Creating a Balanced Approach to Online Safety

> The more kids have a say in the decisions around tech, the less likely they'll see Internet safety as a list of rules to overcome.
>
> *Marilyn Evans, founder of Parents Aware*

Starting a conversation about inappropriate apps on your child's phone can be challenging, but it is an important step toward fostering open communication, trust, and responsible digital behavior.

According to the American Academy of Child and Adolescent Psychiatry, children ages 8–12 in the United States spend 4–6 hours a day on average watching or using screens, and teens spend up to 9 hours a day.[18]

So … How Do I Start That Conversation?

When kids enter the teen years, you (parents and trusted adults) still have some influence, but peer influence is a big deal. At this age, kids are becoming more autonomous online. If they want to find something, they'll find it. So, they need to know there's a safe place at home where they can ask important questions. Often, kids are afraid that if they do, they'll get in trouble and lose their tech. Their fear of losing access to the phone can override their desire to talk about what's going on.

The goal of these conversations is to raise critical consumers of technology. When the focus remains on blocking content, kids simply are not learning how to make decisions on their own. Eventually, they will find ways around filters and parental controls. Family safety meetings can become a regular part of your tech routine — and another low-pressure way to talk about online safety together.[19]

Conversations based on fear may send the wrong message to your child. Start with having small conversations often about the topic of online safety to help them feel safe talking to you about this subject. Ask questions about what they learn in school about online safety or what rules their friends have and how they differ.

Ask them to show you which apps they spend the most time on, what they like about the apps, and if anything, ever makes them feel uncomfortable. Exploring together can foster natural discussion or teaching opportunities.

Engage your child in conversations about their hobbies and interests to guide them toward age-appropriate websites and apps that align with their passions. As they grow, periodically revisit and assess these sites together to ensure they continue to be safe and suitable.

When exploring new apps or websites, consider using them together to foster a shared understanding of online safety and appropriateness. This approach helps maintain an open dialogue while ensuring your child navigates the Internet responsibly.

If your child has it, you should have it. That simple principle can go a long way in protecting your children. If you don't know a lot about a certain game or app, download it on your phone and look through the different features. Assume that all apps have messaging capabilities. This will help you better understand potential opportunities for predators to contact your child.[20]

The following are five questions that parents, a trusted adult, and if appropriate an educator can use to guide an understanding of potential risks and teach your children, tweens, and teens how to identify suspicious behavior and to be cyber-safe while online.

1. Do you know who you're talking to?

   This question encourages tweens/teens to think critically about online contacts. Predators often disguise their identities, so individuals should avoid sharing personal information with people they don't know in real life.

2. Has anyone asked you to keep secrets online?

   Predators may try to build trust by asking their online "friends" to keep their communication private. It's important to stress that trusted relationships are open, and secrecy should be a red flag.
3. Do they ask you for personal information or pictures?

   This question highlights the dangers of sharing sensitive information. Your children should understand that no one online should be asking for personal details or photos, especially people they've never met.
4. Have you been asked to meet someone in person that you only know online?

   Predators may attempt to move online interactions into the real world. Discuss the risks associated with this and explain that under no circumstances should they ever agree to meet someone from the Internet without discussing it with a trusted adult first.
5. Do you feel uncomfortable or unsure about something someone said or did online?

   Encourage children to listen to their instincts. If something feels off or makes them uncomfortable, they should know it's okay to stop the interaction and talk to a parent, guardian, trusted adult, or teacher about it.

These questions can help create an ongoing dialogue about online safety and ensure that children/tweens/teens feel comfortable coming forward if something seems wrong.

Downloading Apps without Permission

The question becomes is the downloading of the unauthorized/unapproved app the issue or that your child attempted to hide this action?

A discussion should first start with addressing the keeping of secrets from you and disobeying Internet appropriate rules set (you have set those correctly?). Don't make this discussion about the technology (i.e., the phone). You may wish to instead turn the discussion to ask how your child would feel if you lied to her/him. How might this affect the future relationship between you two? How does your child feel about lying to you?

Having a phone in today's digitally dependent society is for most people a necessity … most people, but not everyone. Or at least not a wide-open, unsupervised smartphone.

There needs to be honest conversations around the use of the phone because that's how you and those you care for compromise on the unsafe aspects of it.

Additional Protective Measures for a more Cyber-Safe Online Experience

Further actions to increase cyber-safe practices would be to lock down the device using parental controls within screen time settings to restrict future app downloads or usage.

The use of application software to accomplish this is both prudent and proactive if, after discussions, your concerns are still heightened.

Google Family Link is a software tool designed to help parents, caregivers, and trusted adults manage their children's online experience. Google Family Link controls the apps and content that children can access, trusted adults, caregivers, etc., the ability to set screen time limits, monitor app usage, and approve or block app downloads. Family Link also enables trusted adults to view real-time activity reports, giving them insights into how much time a child spends on different applications or websites. This helps ensure children are engaging with content that aligns with family guidelines and safety standards.

One of the most useful features of Family Link is the ability to set daily screen time limits and enforce bedtime schedules, which can help create a balanced approach to technology use. Adults can remotely lock the child's device when it's time for homework or family activities. Additionally, Family Link allows for location tracking of a child's device, ensuring caregivers know where their children are while using their phones or tablets.

The app supports multiple types of devices, making it accessible across a range of platforms. It also offers tools for managing access to mature or inappropriate content, giving parents peace of mind by filtering out apps and websites that may not be age-appropriate. While Family Link doesn't entirely restrict everything a child may encounter, it provides a robust framework for maintaining oversight and promoting safer online habits.

Google Family Link is one of many application software tools available to assist parents, caregivers, trusted adults, etc., in monitoring mobile phone online activity. Table 2.6 provides a list of app tools similar to Google's Family Link designed to assist in monitoring the online experiences of users under the age of 18.

Table 2.6 App Monitoring Tools

APP NAME	VENDOR/ORGANIZATION	DESCRIPTION
Apple screen time	Apple Inc. https://support.apple.com/en-us/108806	Provides insights into app usage, screen time limits, and downtime scheduling. Parents can control what apps their children use, set time limits, and filter age-inappropriate content.
Aura	Aura Parental Controls (previously known as Circle) https://meetcircle.com	Allows parents to manage screen time and filter content across all devices connected to the home Wi-Fi network.
Bark	Bark Technologies www.bark.us/?srsltid=AfmBOor64l5jRQhhqs4mjfJ4Lx6bcd2sgUjRSrDGc_EWFU9LtdEaeeAE	Monitors texts, emails, and social media for potential risks. Alerts parents to issues like cyberbullying, predators, or inappropriate content.
ESET parental control	ESET www.eset.com/int/home/parental-control-android/	Provides content filtering, time management, and real-time location tracking for children's devices.

(*Continued*)

Table 2.6 (*Continued*) App Monitoring Tools

APP NAME	VENDOR/ORGANIZATION	DESCRIPTION
FamiSafe	Wondershare https://famisafe.wondershare.com	Offers app monitoring, location tracking, web content filtering, and screen time management to ensure online safety.
Kaspersky safe kids	Kaspersky Lab https://usa.kaspersky.com/safe-kids	Includes real-time location tracking, web filtering, app usage controls, and allows parents to monitor social media activity.
Microsoft family safety	Microsoft Corporation www.microsoft.com/en-us/microsoft-365/family-safety	Allows parents to manage screen time, set app and game limits, and monitor their children's online activity. It also includes location sharing and driving reports for safety.
Mobicip	Mobicip, LLC www.mobicip.com	Features content filtering, app blocking, screen time limits, and location tracking across multiple platforms.
Norton family	NortonLifeLock https://tinyurl.com/Norton-Control	Provides web filtering, time supervision, and activity reports, helping parents manage what their kids do online.
Qustodio	Qustodio, LLC https://tinyurl.com/d7ntrz2y	Offers content filtering, app monitoring, screen time limits, and social media tracking for parents.
Screen time	Screen Time Labs https://screentimelabs.com	Allows parents to set daily screen time limits, block certain apps, and view their children's activity on mobile devices.
WebWatcher	Awareness Technologies www.awarenesstechnologies.com	Monitors texts, social media, and browsing history, and allows parents to track location and block inappropriate content.

Be Proactive, Be Cyber-Safe

While parental controls offer a valuable layer of protection, they should not be a substitute for open, honest discussions with your child. These conversations can build trust and give children the tools to navigate online risks independently.

Start by explaining what inappropriate content is and why it may be harmful. Ask your child about their experiences and how they've handled any uncomfortable situations. This can give you further insight into their online behavior and reassure them that you're there to help without judgment.

Work together to understand how to report inappropriate content and emphasize that you're always available for support. Children may hesitate to share concerns out of fear of getting in trouble, so regular, open communication helps create a safe space for them to come to you whenever something goes wrong online.

Readers are directed to Appendix F: Hidden Dangers: Identifying Risky Apps on Your Child's Device, for additional information and a step-wise process for examining Apple and Android devices for potentially hidden and/or inappropriate apps.

Password Security and Account Protection

In reaching students to discuss this important cyber-safe topic, educators should stress the importance of creating strong, unique passwords and the necessity of regularly updating them. Discussions should also include the benefits of using two-factor authentication (2FA).

Weak passwords are a common entry point for threat actors, and too many individuals make it too easy for them to gain access to sensitive, personal, and private information. Teaching students about password security assists them in protecting their accounts from unauthorized access, thereby safeguarding their personal information and online activities. It also instills good digital habits and cyber-safe practices.

Teaching students to be proactive and to take charge of their online presence and control over their personal private information (PPI) is an important lesson and in today's digital world a necessary skill.

Educators may wish to begin discussions with their students about the necessity of keeping their private information private and secure. Discussions should focus on the following means by which students can keep private information private and themselves cyber-safe.

Use Strong Passwords or Even Stronger Passphrases

The concept of using strong passwords, even better passphrases, is also discussed in Chapter 1. The following information adds to the discussion in Chapter 1 and provides additional perspective and material that an educator can use to reinforce to students the necessity of establishing strong access controls (i.e., passwords and passphrases).

Always use a combination of letters, numbers, and symbols in your passwords. Think of your favorite game characters and use initials and special characters to make it strong, like "M@ri0C@rt2024."

While passwords have been used as a means of mitigating unauthorized access to private information and files, the rapid advances and application of artificial intelligence (AI) to guessing passwords are making the use of a password, less and less secure as a means of protecting what you want to keep safe, secure, and private.

Students should be encouraged to use a passphrase instead of a password when trying to secure their private data.

A passphrase is similar to a password in usage but is generally longer for added security, usually at least 14 characters in length, with spaces between words. Passphrases are the strongest type of passwords and the easiest to remember.

Simply use an entire sentence for your password, such as "Meet UP with Tony t0 play Splatoon 3 @ 4!". By using numbers, punctuation, and special characters in place of regular letters, this 41-character passphrase is hard to guess but easy to remember.

Enable Two-Factor Authentication

2FA is another method of identity validation layered on a traditional identity and password (lock and key) access method, which offers several benefits:

- Provides an extra layer of security for individuals and systems where it has been applied, reducing the risk of unauthorized access.

- Protects the people who have data in the system by allowing only those with legitimate business purposes to access that data, preventing criminals from using it for fraudulent purposes.
- Ensures that you are the only person who can access your account, even if someone knows your password.

2FA requires the additional step of entering a passcode with a username and password/passphrase, making it much more difficult for someone with bad intent to obtain login information and access private data (see Figure 2.1). There are multiple ways a passcode can be provided, including through the vendor app, a text message, a phone call, or through the use of a hardware token.[21]

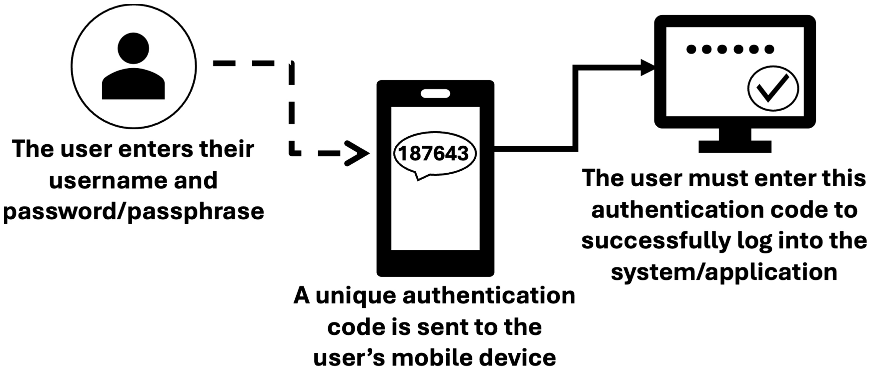

The user enters their username and password/passphrase
187643
A unique authentication code is sent to the user's mobile device
The user must enter this authentication code to successfully log into the system/application

Figure 2.1 Privacy via two-factor authentication (2FA).[22]

Always turn on 2FA to add an extra layer of security! Think of 2FA as needing a second verifiable code to open and give you access to your phone.

Recommendations for Implementing Two-Factor Authentication

Implementing 2FA is a key security measure for protecting one's accounts.

When planning a discussion on the importance of implementing 2FA, educators may wish to stress the following key benefits to assuring that students enable 2FA on their mobile devices.

1. Enhanced Security: 2FA adds an extra layer of security beyond just a username and password. Even if threat actors obtain login credentials (e.g., through phishing or data breaches), they would still need the second factor (usually something only the user has, such as a mobile phone or hardware token) to access the account.
2. Mitigates the Risk of Password-related Attacks: Common attacks like brute force, credential stuffing, or password guessing are rendered ineffective if 2FA is in place. Even strong passwords can be vulnerable to these attacks, but requiring a second form of authentication adds significant protection.
3. Reduces Impact of Data Breaches: When large-scale data breaches occur, leaked credentials are often sold or reused across multiple sites. With

2FA enabled, these leaked credentials cannot be used to access a student's account without the additional factor, greatly limiting the damage from such breaches.

4. Protection against Phishing: Phishing attacks aim to steal credentials by tricking users into entering them on fraudulent sites. 2FA helps mitigate the success of such attacks because, even if users accidentally provide their username and password, attackers won't have access to the second factor, which is typically a time-sensitive code. See the following Recognizing and Avoiding Phishing Scams section, for additional insights to provide to students on maintaining a cyber-safe presence while online.

Recognizing and Avoiding Phishing Scams

Phishing involves deceptive attempts to obtain sensitive information, often through email or fake websites. This topic educates students on identifying and taking measures to successfully avoid these scams.

As phishing attacks become more sophisticated, students must recognize the signs of a scam. Early education helps them avoid falling victim to identity theft and unauthorized access to personal, private information. This awareness is critical as students begin to engage more with online content and with less supervision.

Educators … teach your children well. Teach them to be cautious of emails or messages asking for personal information. If they receive a text, email, or voicemail saying they won a new gaming console but need to share their password, it's likely a scam.

Alert students that phishing emails and text messages often tell a story to trick them into clicking on a link or opening an attachment. They might get an unexpected email or text message that looks like it's from a company they know or trust, like Mojang Studios, the developers of Minecraft, for example.

Or maybe it's from an online music or gaming website or app. The message could be from a scammer, who might

- say they've noticed some suspicious activity or log-in attempts to the student's account — they haven't;
- claim there's a problem with the student's account or prepayment information on file — there isn't;
- say that the student needs to confirm some personal or financial information — they don't;
- include a bill for a popular game software upgrade they don't recognize — it's fake;
- want the student to click on a link to make a payment, but — the link has embedded malware;
- say that the student is eligible to register for a half-priced, advanced, prerelease copy of the next major gaming software product — it's a scam;
- offer a coupon for free stuff — it's not real.

Phishing Scams: 10 Red Flags

Listed below are 10 "red flags" to discuss with students. Students should be made aware of these "red flags" when examining an email to determine if it is legitimate or from a scammer.

1. Suspicious Email Address: Check the sender's email address carefully. Scammers often use addresses that look similar to legitimate ones but may have subtle differences, like extra characters or misspelled domains (e.g., support@paypall.com instead of support@paypal.com).
2. Generic Greetings: Fake emails often use generic greetings like "Dear Customer," "Dear User," "Hi," or "Hello" instead of addressing you by name. Most legitimate companies will use your real name if you've interacted with them before.
3. Urgent or Threatening Language: Scammers create a sense of urgency by threatening account suspension, legal action, or other dire consequences if you don't click on a link or respond immediately.
4. Unsolicited Attachments or Links: Be wary of emails with unexpected attachments or links, especially if they are urging you to click. They may contain malware or lead to phishing sites.
5. Grammatical and Spelling Errors: Scam emails often contain awkward grammar, poor spelling, and strange sentence structures. Legitimate companies typically proofread their communications. Be aware, be cautious … with the growing use of AI, scammers are using AI to produce emails that are linguistically and grammatically correct and culturally accurate, making these fake emails seem to be all too real!
6. Requests for Personal Information: Legitimate companies rarely ask for sensitive information like passwords, Social Security numbers, or credit card details via email. If an email requests this, it's a big red flag.
7. Unusual Requests: Be vigilant if the email asks for something out of the ordinary, such as wiring money, purchasing gift cards, or sending financial details to resolve a problem.
8. Too Good to Be True Offers: If the email offers something that seems too good to be true (e.g., huge prizes, free giveaways, or large sums of money), it's probably a scam.
9. Suspicious URLs: Hover over any links in the email without clicking. Scammers often use links that look legitimate but redirect to malicious websites. Check if the URL matches the official domain.
10. Missing Contact Information: Legitimate companies usually include full contact information in their emails, such as a business address, phone number, and support email. A lack of this information or vague details is a red flag.

Scammers/threat actors employ phishing techniques to get you to click on a link or download an attachment that may contain malicious software (malware).

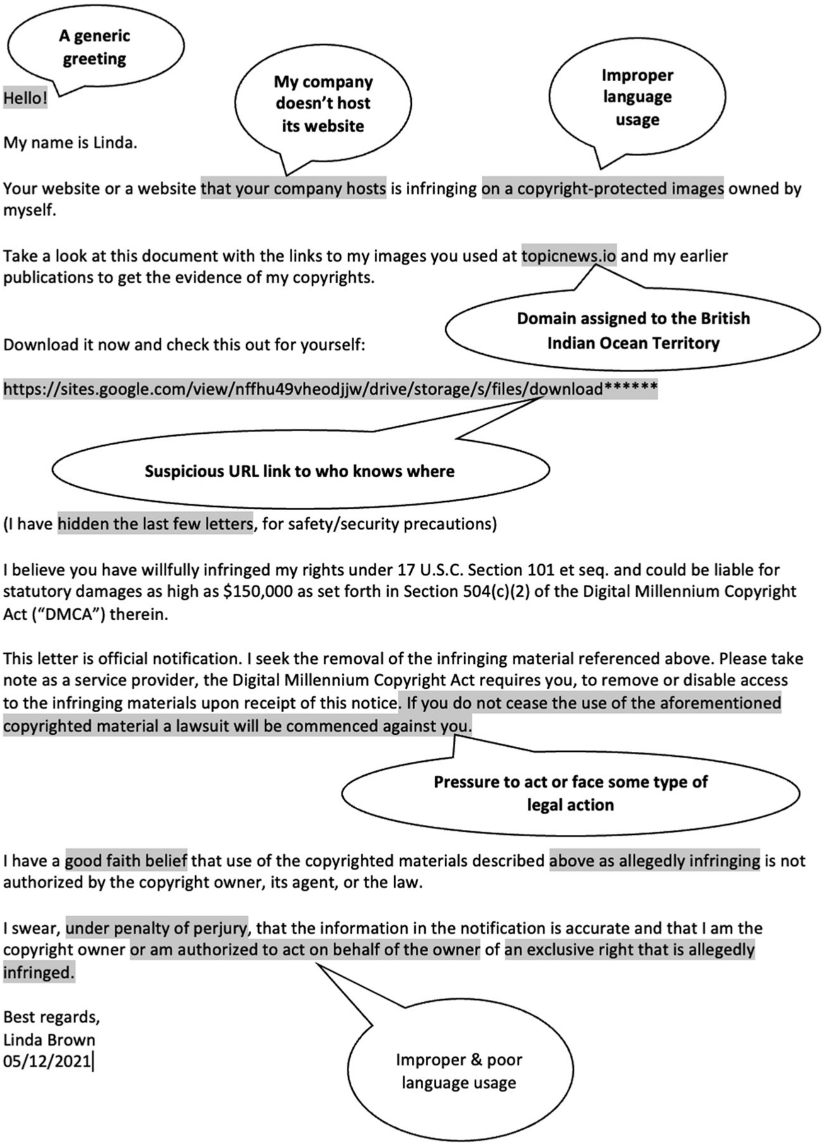
A social media site that looks legitimate can hide malicious embedded web links that can secretly redirect users to other sites. If you are unsure of something, navigate directly to the site or use a search engine instead of clicking the link.

Be careful of web links embedded on a user page. Enable anti-spam and anti-phishing security features. Domain checkers can be useful to gauge the origin of the unknown link.

Activity

Figure 2.2 is an example of a scammer's email that was sent in an attempt to extort money from the recipient.

Use this figure in class exercises or discussions with students, as it highlights several "red flags" that identify an email (or text) that may be from a scammer.



Hello!

My name is Linda.

Your website or a website that your company hosts is infringing on a copyright-protected images owned by myself.

Take a look at this document with the links to my images you used at topicnews.io and my earlier publications to get the evidence of my copyrights.

Download it now and check this out for yourself:

https://sites.google.com/view/nffhu49vheodjjw/drive/storage/s/files/download******

(I have hidden the last few letters, for safety/security precautions)

I believe you have willfully infringed my rights under 17 U.S.C. Section 101 et seq. and could be liable for statutory damages as high as $150,000 as set forth in Section 504(c)(2) of the Digital Millennium Copyright Act ("DMCA") therein.

This letter is official notification. I seek the removal of the infringing material referenced above. Please take note as a service provider, the Digital Millennium Copyright Act requires you, to remove or disable access to the infringing materials upon receipt of this notice. If you do not cease the use of the aforementioned copyrighted material a lawsuit will be commenced against you.

I have a good faith belief that use of the copyrighted materials described above as allegedly infringing is not authorized by the copyright owner, its agent, or the law.

I swear, under penalty of perjury, that the information in the notification is accurate and that I am the copyright owner or am authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

Best regards,
Linda Brown
05/12/2021

A generic greeting
My company doesn't host its website
Improper language usage
Domain assigned to the British Indian Ocean Territory
Suspicious URL link to who knows where
Pressure to act or face some type of legal action
Improper & poor language usage

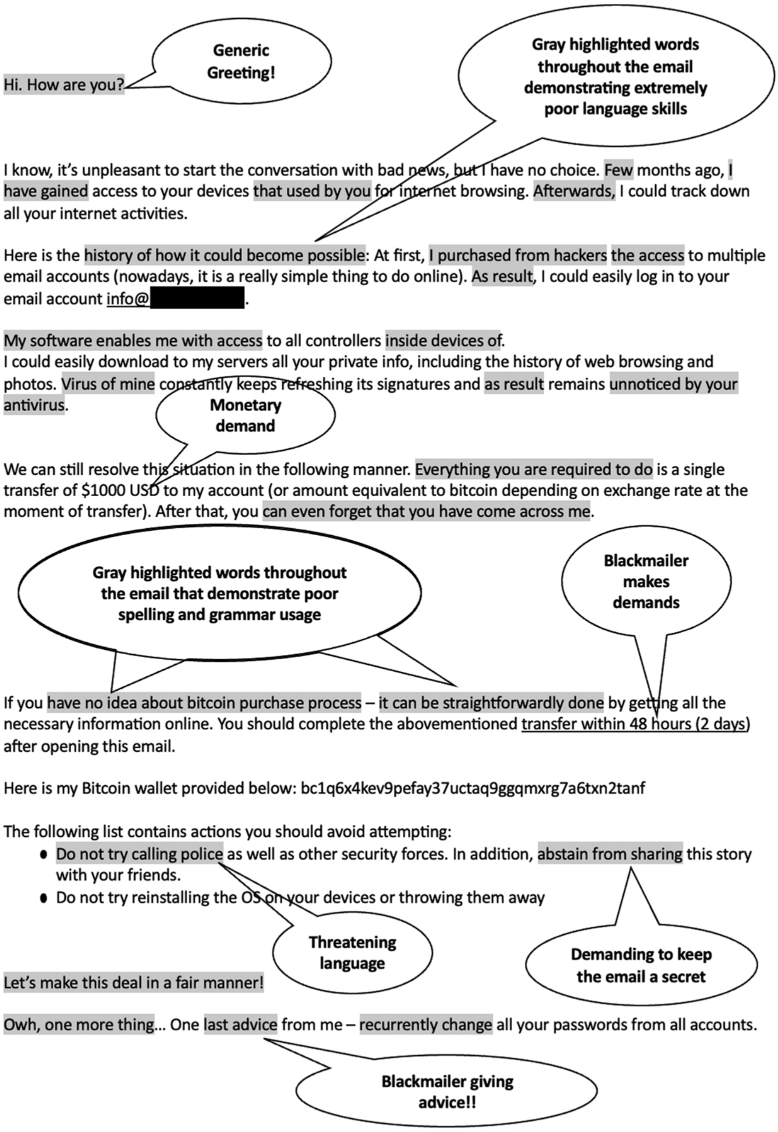
Figure 2.2 Example phishing email.[23]

The Darker Side of Phishing Scams

It is important to have frank and honest discussions with your students and parents with your children … phishers can resort to blackmail!

After successfully obtaining sensitive information, such as compromising photos, personal conversations, or even financial data, scammers may threaten to release or misuse this information unless the victim pays a ransom. This is often referred to as sextortion when it involves private or intimate material. See a further discussion on this topic in Chapter 3.

Blackmail in phishing scams is a serious risk that can lead to both emotional and financial distress for victims. Figure 2.3 is an example of a scammer's email that was sent attempting to blackmail the recipient.



Hi. How are you?

I know, it's unpleasant to start the conversation with bad news, but I have no choice. Few months ago, I have gained access to your devices that used by you for internet browsing. Afterwards, I could track down all your internet activities.

Here is the history of how it could become possible: At first, I purchased from hackers the access to multiple email accounts (nowadays, it is a really simple thing to do online). As result, I could easily log in to your email account info@[redacted].

My software enables me with access to all controllers inside devices of.
I could easily download to my servers all your private info, including the history of web browsing and photos. Virus of mine constantly keeps refreshing its signatures and as result remains unnoticed by your antivirus.

We can still resolve this situation in the following manner. Everything you are required to do is a single transfer of $1000 USD to my account (or amount equivalent to bitcoin depending on exchange rate at the moment of transfer). After that, you can even forget that you have come across me.

If you have no idea about bitcoin purchase process – it can be straightforwardly done by getting all the necessary information online. You should complete the abovementioned transfer within 48 hours (2 days) after opening this email.

Here is my Bitcoin wallet provided below: bc1q6x4kev9pefay37uctaq9ggqmxrg7a6txn2tanf

The following list contains actions you should avoid attempting:

- Do not try calling police as well as other security forces. In addition, abstain from sharing this story with your friends.
- Do not try reinstalling the OS on your devices or throwing them away

Let's make this deal in a fair manner!

Owh, one more thing… One last advice from me – recurrently change all your passwords from all accounts.

Generic Greeting!
Gray highlighted words throughout the email demonstrating extremely poor language skills
Monetary demand
Gray highlighted words throughout the email that demonstrate poor spelling and grammar usage
Blackmailer makes demands
Threatening language
Demanding to keep the email a secret
Blackmailer giving advice!!

Figure 2.3 Example blackmail email.[24]

Note to the reader … the email used in this example is real! Several details have been removed from the original email due to the vulgar language used by the scammer, language that is inappropriate to include in this book, as it does not contribute to any substantiated education or learning … for the student or the educator.

Activity

Use this figure in class exercises or discussions with students, as it highlights several of the "red flags" that identify this email is from a scammer.

If you see that a friend or family member may be compromised, reach out to them through other means and ask them to verify any posts you think might be fraudulent.

That way, if they've been compromised, they can take the necessary steps to regain control of their accounts. A compromised account can be used to compromise other accounts, so be aware of "friends" posting in suspicious ways.

Pig Butchering Scam

This scam is named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies. The scam is also known as "Killing Pig Plate" or "Sha Zhu Pan."

So, now you must be wondering… "Why did the authors include this topic in a book aimed at teaching middle school students to be cyber-safe?"

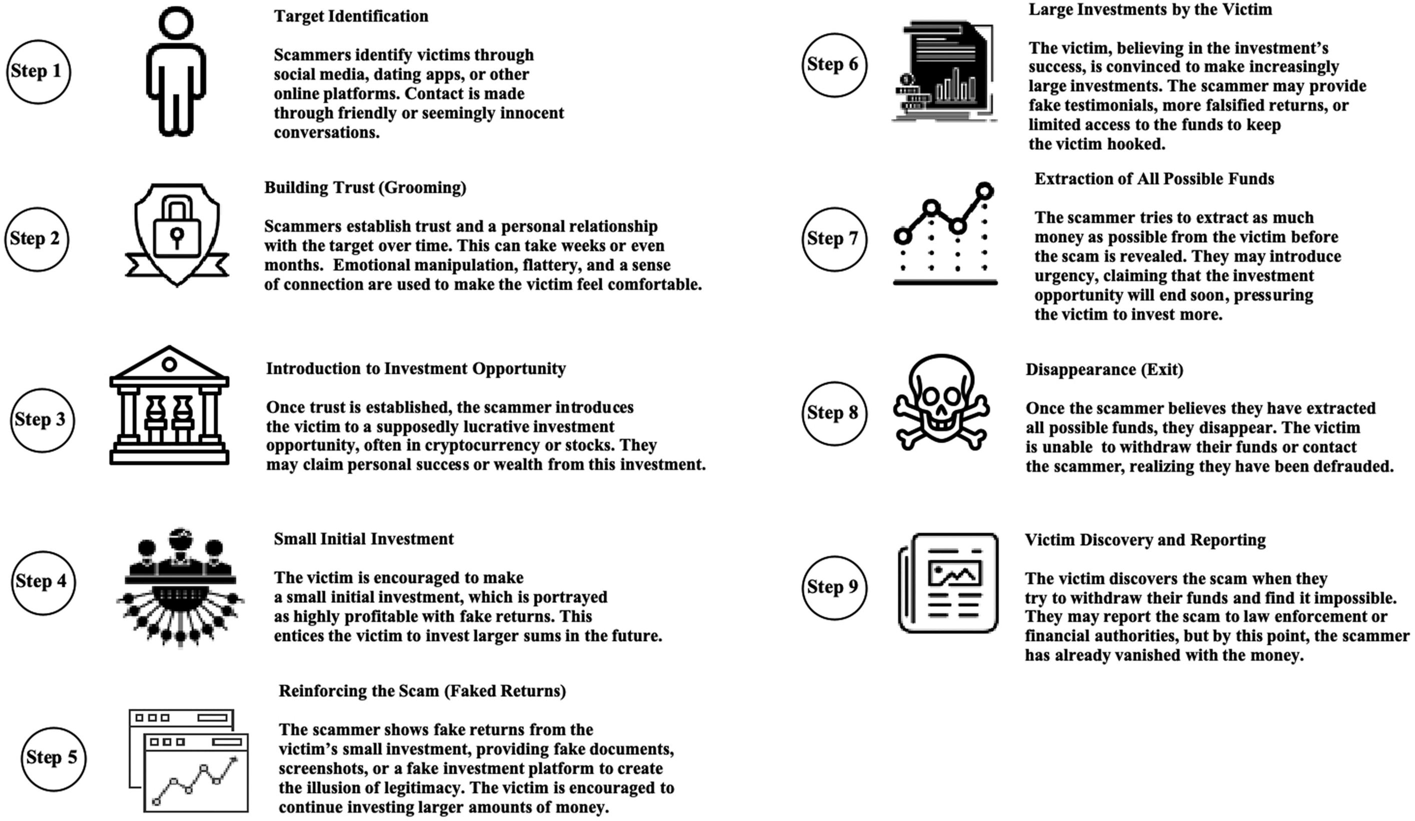
The topic has been included in this section, not for students primarily but for you, the reader. Teaching students to be cyber-safe in our digital world is an essential skill they must hone and practice. As an adult, being cyber-vigilant and cyber-safe is a constant endeavor, and we must lead by example!

How Do You Butcher a Pig?

This is how a pig butchering scam works:

1. Perpetrators will contact you out of nowhere via text messages, dating apps, and social media platforms, and later switch to Voice over Internet Protocol (VoIP) chat applications.
2. Perpetrators will try to develop meaningful relationships with you, gain your trust, and offer you high-yield investment opportunities in virtual assets, such as cryptocurrency.
3. Perpetrators will tell you to open accounts on online investment websites and instruct you to deposit money via wire transfer to shell companies, or direct transfers to legitimate virtual asset service providers or cryptocurrency exchanges.
4. Perpetrators will pressure you to invest more money, or your relationship with them will end.
5. You can be duped, and the fraud will end: When you attempt to withdraw money, websites may demand that you pay additional fees to do so, or you may be locked out of the account and never hear back from the perpetrator.
6. Perpetrators disappear with all of your funds.[25]

Figure 2.4 outlines the steps a malicious scammer takes in executing a pig butchering scam.



Step 1

Target Identification

Scammers identify victims through social media, dating apps, or other online platforms. Contact is made through friendly or seemingly innocent conversations.

Step 2

Building Trust (Grooming)

Scammers establish trust and a personal relationship with the target over time. This can take weeks or even months. Emotional manipulation, flattery, and a sense of connection are used to make the victim feel comfortable.

Step 3

Introduction to Investment Opportunity

Once trust is established, the scammer introduces the victim to a supposedly lucrative investment opportunity, often in cryptocurrency or stocks. They may claim personal success or wealth from this investment.

Step 4

Small Initial Investment

The victim is encouraged to make a small initial investment, which is portrayed as highly profitable with fake returns. This entices the victim to invest larger sums in the future.

Step 5

Reinforcing the Scam (Faked Returns)

The scammer shows fake returns from the victim's small investment, providing fake documents, screenshots, or a fake investment platform to create the illusion of legitimacy. The victim is encouraged to continue investing larger amounts of money.

Step 6

Large Investments by the Victim

The victim, believing in the investment's success, is convinced to make increasingly large investments. The scammer may provide fake testimonials, more falsified returns, or limited access to the funds to keep the victim hooked.

Step 7

Extraction of All Possible Funds

The scammer tries to extract as much money as possible from the victim before the scam is revealed. They may introduce urgency, claiming that the investment opportunity will end soon, pressuring the victim to invest more.

Step 8

Disappearance (Exit)

Once the scammer believes they have extracted all possible funds, they disappear. The victim is unable to withdraw their funds or contact the scammer, realizing they have been defrauded.

Step 9

Victim Discovery and Reporting

The victim discovers the scam when they try to withdraw their funds and find it impossible. They may report the scam to law enforcement or financial authorities, but by this point, the scammer has already vanished with the money.

Figure 2.4 Steps in conducting a "Pig Butchering" scam.[26]

A Scenario Designed for Student Discussion and Engagement

Educators, the following scenario has been provided as the basis for ongoing discussions with your students. Scammers who have previously targeted adults are expanding their reach, morphing their scams, and now seeking to entrap new victims. Don't let your students become a victim!

Teaching Tip

Lily, a 13-year-old middle school student, enjoys playing online games and connecting with new people through social media. One day, she receives a friendly message on Instagram from someone named "Jason," who claims to be a 14-year-old gamer with similar interests. Over a few weeks, they chat frequently, discussing school, hobbies, and games. "Jason" often compliments Lily on her gaming skills and builds a sense of trust, making her feel valued and special.

After a month, "Jason" tells Lily about a new online game that also allows players to earn real money by investing small amounts of money in digital currency. He shows her screenshots of his own supposed earnings, which appear impressive. Jason convinces Lily to try it out, telling her that she could earn enough to buy better in-game items or even help her family with expenses.

Lily, intrigued and excited, tells her parents she needs $20 for a new game, which they give her. She invests it in the platform Jason recommended. The platform, run by scammers, shows her initial "profits" growing, and Jason encourages her to invest more to earn bigger rewards. Lily begins asking for more money from her parents for different excuses, like school projects or in-game purchases. Over time, her investments total $200.

However, when Lily tries to withdraw her funds from the platform, she is unable to. Jason suddenly becomes unresponsive. Lily realizes too late that she has been scammed, losing not only her own money but also what her parents had given her.

Activity

The following are open-ended discussion questions that an educator could use to initiate a "discussion for learning" based on the scenario provided:

These questions can be used for either in-class group discussion or assigned for out-of-class work. Richer learning outcomes will be achieved when students are allowed to discuss the questions and peer responses in an open, honest, and safe environment.

1. How do you think Lily felt when she first started talking to "Jason"? What made her trust him, and do you think that trust was justified?
2. Why do you think "Jason" shared the investment opportunity with Lily? What would you do if a new online friend offered you a similar chance to make money?
3. What signs or red flags in Lily's situation might have indicated that something wasn't right? Can you think of other examples of situations where someone online might try to trick you?

4. Why is it important to talk to a trusted adult, like a parent or teacher, before making decisions about money or sharing personal information online?
5. If you were Lily's friend, what advice would you give her before she decided to invest her money? How could friends help each other stay safe online?

Educator Takeaways from the Scenario Activity

There are three important takeaways from this activity that educators should be aware of, as they continue discussing cyber-safety habits with their students.

- Emotional Manipulation: Middle school students are easily drawn into online friendships and are vulnerable to emotional manipulation. They might trust someone they've never met due to their lack of experience.
- Financial Naivety: Students in this age group often don't fully understand the complexities of investments or scams, making them susceptible to "easy money" schemes.
- Pressure to Keep Up with Peers: Social pressure to get better items in games or to "fit in" can drive children to take risks, including trusting the wrong people or making poor financial decisions.

Being aware of, exposed to, and prepared to avoid such scams makes you better able to relate these risks to your students.

True, many middle school students may never be directly targeted by such a scam; however, their loved ones may. Discussing these types of scams with students arms them with additional knowledge to remain proactive in sustaining a cyber-safe presence in their online world.

Stay Cyber-Safe: Don't Take the Bait

The Cybersecurity and Infrastructure Security Agency (CISA), within the US Department of Homeland Security, and the NCDIT provide the following tips for staying safe and recognizing phishing that can be shared with students.

1. Recognize

   Look for these common signs:

   - Urgent or emotionally appealing language, especially messages that claim dire consequences for not responding immediately
   - Requests to send personal and financial information
   - Untrusted shortened URLs
   - Incorrect email addresses or links, like amazan.com.

   A common sign used to be poor grammar or misspellings, although in the era of AI, some emails will now have perfect grammar and spelling, so look out for the other signs.

2. Resist

   Advise students that if they suspect phishing, resist the temptation to click on links or attachments that seem too good to be true and may be trying to access their personal information. Instead, report the phish to protect themselves and others.

Means and avenues to report phishing scams can vary by State, city, school district, etc. Students should be advised to report phishing scams to a parent, or trusted adult, when and if appropriate a teacher. Alert students that they may also contact the Federal Trade Commission [www.consumer.ftc.gov/features/feature-0014-identity-theft] or by calling 1–877-IDTHEFT. (Text added by authors)

3. Delete: Delete the message. Don't reply or click on any attachment or link, including any "unsubscribe" link. Just delete.[27]
4. Think before You Act: Be wary of messages that implore you to act immediately, offer something that sounds too good to be true, or ask for personal or financial information.
5. When in Doubt, Throw It Out: Cybercriminals often use links in emails and online posts to try to gain access to devices. If a message seems suspicious — even if you know the source — it is best to delete it or report it as spam.
6. Follow-up: Email and social media scams can be elaborate. If a message from a known sender seems out of the ordinary, check with the sender or poster using another method of communication.
7. Visit and Download Information Only from Trusted Sources: Carefully inspect websites you are unfamiliar with to be sure they are legitimate.
8. Use Stronger Authentication: Enable multifactor authentication, when available, to help verify authorized access to online accounts.
9. Make Passwords Long and Strong: Combine capital and lowercase letters with numbers and symbols to create a more secure password.
10. Avoid Clicking Links in Suspicious Messages: Instead, use a reputable search engine to get to the site or type the URL directly into your browser. If you choose to click a link, first verify its authenticity by hovering your cursor over the link to reveal the full address.
11. Do Not Reply to Spam or Click "unsubscribe" Links in Emails: Doing so could confirm to the sender that your email address is valid or lead to malware being installed on your device. Instead, report the message as spam.
12. Connect Only to Trusted Networks: Use a reputable network VPN when connecting to public Wi-Fi. If you have a hotspot on your mobile device, use that instead. Unknown networks may not be secure and can allow threat actors access to your devices.
13. Install and Update Antivirus Software: Make sure your devices are equipped with regularly updated antivirus software, firewalls, email filters, and anti-spyware.

14. Keep Software up to Date on Your Devices: Reliable developers keep their products up to date to protect against online threats. Contact the service desk if you have difficulty installing updates.
15. Check Privacy Policies: Before submitting your email address (or any other personal information) online, read the site's privacy policy so you know how your information will be used.[28]

    Additional tips to discuss with students directly aimed at protecting their information and reducing the success of a phishing attack.
16. Keep a Low Profile: Reduce the amount of personal information you post online (e.g., phone numbers and address.)
17. Verify the Caller: If you receive a call from a retail store where you just purchased an item, hang up and call them back to verify the legitimacy of the call and the person calling.
18. Verify Links before You Click Them: Hover over the link to see if the info (sender/website address) matches what you expect.
19. Suspicious Attachment Alert: Be wary of unexpected attachments that you didn't request as these are a major sign of a phishing attempt. Never download or open these attachments.
20. Recognize Unfamiliar Greeting: A generic greeting, like "Dear User" or "Hi," is often a sign of a phishing email. Some phishing emails don't include a greeting at all.

Continually discuss with students the reality and necessity of remaining vigilant and cyber-safe before clicking, opening, or responding to emails and texts, especially from an unknown, unrecognized source.

Understanding Digital Footprints

This topic discusses how every online action leaves a digital trail, which can be traced and potentially accessed by others, including future employers and colleges.

Students often don't realize that their online actions can have long-term consequences. Understanding digital footprints helps them make informed decisions about what they share online, promoting a positive digital presence that will benefit them in the future.

Pew Research Center analysis shows just how fleeting online content is:

- A quarter of all webpages that existed at one point between 2013 and 2023 are no longer accessible, as of October 2023. In most cases, this is because an individual page was deleted or removed on an otherwise functional website.
- For older content, this trend is even starker. Some 38% of web pages that existed in 2013 are not available today, compared with 8% of pages that existed in 2023.

- Nearly one in five tweets are no longer publicly visible on the site just months after being posted. In 60% of these cases, the account originally posted the tweet was made private, suspended, or deleted entirely. In the other 40%, the account holder deleted the individual tweet, but the account itself still existed.[29]

Despite the limited lifespan of many posts, tweets, and other digital content, students should be aware of the long-term implications of their digital footprint. Online content can disappear or become inaccessible due to "digital decay," but a significant portion of digital data, including posts or personal information, remains online for years. Even when content is removed, cached versions or archived copies can persist. Moreover, digital traces left behind can be stored, shared, or exploited without one's knowledge. Therefore, students need to understand that their online actions may have lasting consequences on their personal, academic, and professional lives.

The nature of some social platforms and apps is to make it as easy as possible to share private information or locations. Children and teens must understand what is safe to share and what should be kept private.

There is an elevated risk of more visual-based apps used by tweens and teens to broadcast home locations and clues to places they frequently hang out. If this information is public, predators can start understanding what vulnerabilities an individual has and what they enjoy doing, making it easier to make a connection with them over a chat or direct message.[30]

Monitoring Your Cyber Footprint

Encourage your students to search for themself online to determine what information about them is already easily available to a threat actor. It is critical to know what information can be found by a free, open-source search, as it is likely the threat actor's first step in reconnaissance.

Advise students to disallow tagging, as friends may not be as diligent with their location settings. Advise students to be wary of information they post about themselves on their profile and the profiles of close friends and family. Photos and information friends post about the student may reveal the student's critical/sensitive information. This includes warning students not to post pictures of themselves (or family members or friends) while still on vacation, traveling, enjoying a meal at a favorite restaurant, etc.

Managing One's Digital Footprint

The Our Rescue organization's 2024 publication, "Start Talking: A Guide to Keeping Children Safe Online," identified several targeted tips that educators may want to both discuss in class with students and incorporate into out-of-class exercises.

Teaching Tip

These tips for managing your digital footprint include the following:

- Use privacy settings to safeguard your personal photos and videos.
- Remove any content that may misrepresent you.
- Delete old accounts, especially public accounts.
- Look through what others have shared about you.
- Determine what you are comfortable with others sharing about you online.
- Ask others for permission before sharing their photo publicly.
- Avoid posting photos that show your address or typical schedule.[31]

Educators may also wish to incorporate information from Table 2.7 into class discussions and out-of-class exercises to foster further student awareness of the impact of their digital footprint.

Search engine optimization (SEO) tools extend the lifespan of website content far beyond its initial publication. Search engines theoretically immortalize content, but without optimized search engine visibility, information can digitally decay.[32]

To the students…

Everything you do online leaves a trace, so be mindful. Think of your digital footprint as muddy shoes—wherever you step, you leave a mark. Be sure it's a good one!

Table 2.7 Managing Your Digital Footprint

TALKING POINTS FOR EDUCATORS	REINFORCING EXAMPLES
Online content may not disappear, even if deleted.	Show a video on how websites like the Wayback Machine (https://web.archive.org) archive deleted web pages. Encourage students to search for deleted websites. • How to Use Wayback Machine (Website History) (www.youtube.com/watch?v=W1HL9uw6Axg) • A Short Overview of the Internet Archive Wayback Machine (www.youtube.com/watch?v=u_qSh26F1CA)
Posts, tweets, and texts can be saved and shared.	Organize a role-playing exercise where students pretend to be hiring managers reviewing candidates' old social media posts.
Digital footprints can affect future opportunities (e.g., college admissions, jobs).	Have students research cases where someone's old social media posts negatively impacted their career. Present their findings.
Privacy settings don't guarantee complete protection.	Perform a class experiment where students adjust their privacy settings on a mock platform and analyze how much data are still accessible.
Even if a post is deleted, screenshots or saved copies can still exist.	Facilitate a group discussion about the ethics of sharing screenshots of deleted posts. Should they ever be shared? Why or why not?
Digital decay doesn't mean complete erasure; some data persists.	Share statistics from the Pew Research report (https://tinyurl.com/Pew-Research-Report) showing how many webpages from 2013 are no longer accessible today (38%) but explain how digital data are still often archived elsewhere.

Fake News and Media/Information Literacy

> False information would not have any influence if readers were able to tell that it is false. However, several research studies have conducted experiments to measure the ability of humans to detect false information including hoaxes, fake reviews, and fake news, has shown that humans are not particularly good at discerning false from true information.[33]

Exactly What Is Fake News?

So, what is fake news exactly? Well, after a quick look around the Internet, it turns out that there is no generally agreed-upon definition of fake news.

The Massachusetts Department of Higher Education defines "fake news" as news stories that are false or misleading, without verifiable or accurate facts, quotes, or sources.

The information specialists at the Library of the University of Oregon define fake news as information that is clearly and demonstrably fabricated and that has been packaged and distributed to appear as legitimate news. This narrow definition seeks to distinguish fake news from other types of misleading information by clarifying that the former is patently false and was created and presented in a way meant to deceive consumers into thinking it is real. Fake news refers to a specific piece of information; it does not refer to any particular type of news outlet, individual, or other actor.[34]

Fake news is a term that can mean different things to different people. One must also take into consideration that fake news is often the poster child of misinformation, but the uninformed misrepresentation of facts is its overlooked sibling.[35]

Benjamin Herold, in his article "Students have struggled with fake news for longer than you think," quotes Lawrence Paska, the executive director for the National Council for the Social Studies, a membership association that supports social studies education in K—12 and higher education as stating "Whether reading a printed book, a newspaper article or a Facebook post, it's important that students be able to ask key questions, compare competing claims, assess credibility, and reflect on one's own process of reasoning, according to the group's position statement."

A first step, Paska said, is making sure that both students and teachers have an effective framework for evaluating the credibility of information they encounter.[36]

SIFT (The Four Moves): Sorting Truth from Fiction

Such a framework can be found in the four basic SIFT moves students can use when looking at a source, developed by Michael Caulfield of Washington State University Vancouver (see Figure 2.5).

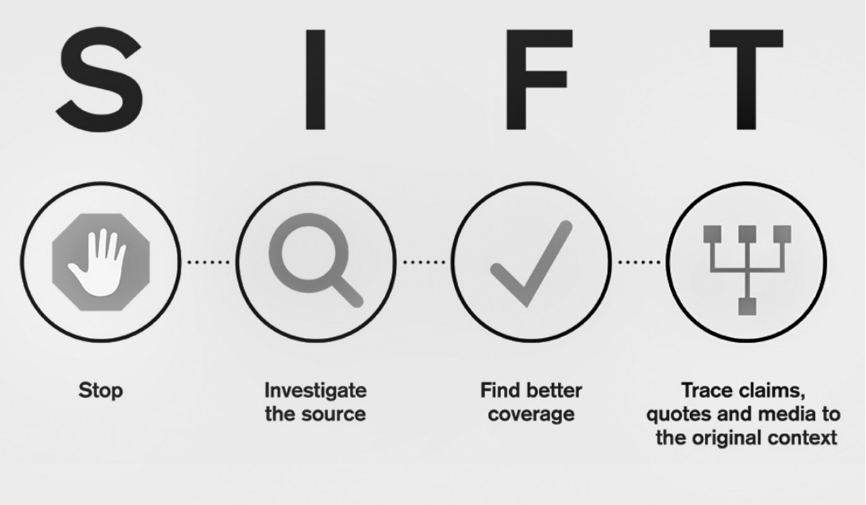


Figure 2.5 SIFT framework.[37]

Caulfield describes the four SIFT moves, which educators may discuss with students:

1. STOP

   The first move is the simplest. **STOP** reminds you of two things.
   - First, when you hit a page or post and start reading it, STOP. Ask yourself whether you know the website or source of the information, and what the reputation of both the claim and the website is. If you don't have that information, use the other moves to get a sense of what you're looking at. Don't read it or share media until you know what it is.
   - If you feel yourself getting overwhelmed in your fact-checking efforts, STOP and take a second to remember your purpose. If you are doing deep research of your own, you may want to chase down individual claims in a newspaper article and independently verify them.
2. Investigate the Source

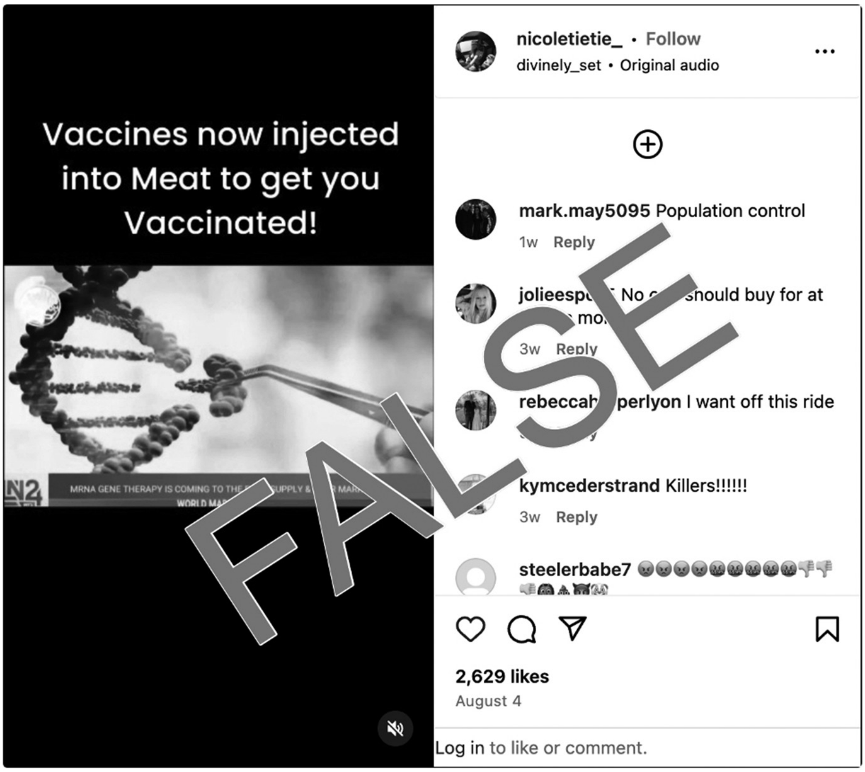
   The idea here is that you want to know what you're reading before you read it.
   - Knowing the expertise and agenda of the source is crucial to your interpretation of what they say. Taking 60 seconds to figure out where the media is from before reading will help you decide if it is worth your time, and if it is, help you to better understand its significance and trustworthiness.
3. Find Better Coverage
   - At times, you don't care about the particular article or video that reaches you. You care about the claim the article is making. You want to know if it is true or false. You want to know if it represents a consensus viewpoint or if it is the subject of much disagreement.

  - The best strategy may be to ignore the source that reached you and look for trusted reporting or analysis on the claim.
4. Trace Claims, Quotes, and Media Back to the Original Context
  - Trace the claim, quote, or media back to the source, so you can see it in its original context and get a sense if the version you saw was accurately presented.

The consistent theme that runs through Caulfield's SIFT framework is that each step is about reconstructing the necessary context to read, view, or listen to digital content effectively.

When evidence is presented with a certain frame — whether a quote, a video, or a scientific finding — sometimes it helps to reconstruct the original context in which the photo was taken, or the research claim was made. It can look quite different in context! In some cases, these techniques will show you claims are outright wrong, or that sources are legitimately "bad actors" who are trying to deceive you.[38]

Using this framework educators can assist students in making decisions when faced with unfamiliar sources and content so they can avoid spending time with misinformation and turn their attention to credible information.


nicoletietie_ • Follow
divinely_set • Original audio
...
MRNA GENE THERAPY IS COMING TO THE
WORLD MA
N2
FALSE
2,629 likes
August 4
Log in to like or comment.

Vaccines now injected into Meat to get you Vaccinated!

mark.may5095 Population control
1w Reply

jolieesp No should buy for at mo
3w Reply

rebeccah perlyon I want off this ride

kymcederstrand Killers!!!!!!
3w Reply

steelerbabe7 😡😡😡😡🤬🤬🤬🤬🤬👎👎

Figure 2.6 Example of a fake news post on Instagram.[39]

Educators may use the example in Figure 2.6, of an Instagram post that falsely states, "Vaccines now injected into Meat to get you Vaccinated!" To carry the message further, the disinformation depicts an image of a DNA strand with a fork suggesting genetic modification. User comments to the post include conspiracy-driven reactions such as "Population control" and "Killers!!!" The post has 2,629 likes!

The takeaway for students … This image promotes vaccine misinformation, implying unethical vaccination practices through food consumption.

Identifying Hoaxes, Fake News, and Rumors in Social Media

Algorithms to identify false information can be broadly categorized into three categories:

1. Feature Engineering-Based
2. Graph-Based
3. Modeling-Based.

The majority of algorithms are feature-based, in that they rely on developing efficient features that individually or jointly can distinguish between true and false information. These features are developed from the characterization analyses that show the differences in properties of the two classes. These differences are then characterized by intelligently designed features.

Alternatively, graph-based algorithms rely on identifying false information by targeting groups of users (spreaders) with unlikely high, lock-step coordination, boosting a certain story (e.g., a botnet retweeting the same article in near-identical time). These algorithms try to identify dense blocks of activity in an underlying adjacency matrix. While these algorithms may be able to identify large-scale coordinated activity, small-scale or lone-wolf attacks are unlikely to be caught since the algorithms primarily focus on the largest, dense blocks.

Modeling-based algorithms work by creating information propagation models that emulate the empirical observation of edges and information spread. The intuition behind these algorithms is that since most information is true, it likely spreads similarly or uniquely. Thus, emulating this mode of information spread can pinpoint false information spread as anomalies, which can then be verified and removed.[40]

Fake News and Misinformation

> Everyone is entitled to his own opinion, but not his own facts.
>
> *Daniel Patrick Moynihan*

As part of your discussion on cyber safety and identifying fake news with students, it is advisable to also cover the topic of misinformation and disinformation, both outcomes of fake news.

Findings from the research survey conducted by the UK Office of Communications released in 2023, showed that children aged 8–17 were less likely to believe information from social media apps or sites compared to other sources they used: a third said that they believed all or most of what they see on social media to be true (32%), while two-thirds thought the same for news apps and sites (66%), and 77% for websites used for school or homework.

However, the level of confidence with which 12–17-year-olds felt they could identify what was real or fake online did not always match their ability. Nearly a quarter (23%) of children claimed to be confident in their ability to identify what is real or fake online but could not correctly identify a fake social media profile when presented with one during the survey.[41]

Table 2.8 provides examples of several types of misinformation accompanying fake news. These information "types" are worth reviewing with your students. The more that students know about spotting fake news, the better prepared they will be to recognize it when they encounter it and be prepared to respond in a cyber-safe way.

Teaching Tip

The Power of AI in Fake News: The Role of Deepfakes

Deepfakes refer to face multimedia content, which has been digitally altered or synthetically created using deep neural networks.[42]

Deepfakes, while commonly associated with face multimedia manipulation, can however also be applied to the following:

- Audio: Deepfakes can synthesize a person's voice, allowing for the creation of realistic speech, often used in impersonation scams or voice manipulation.
- Text: Using AI language models, text-based deepfakes can generate realistic, false written content, mimicking a particular person's writing style or fabricating entire documents.
- Video: Beyond just facial alterations, deepfakes can modify entire video scenarios, including background settings, movements, and other visual elements.
- Images: Deepfakes can be used to create entirely fabricated images or alter existing ones, manipulating objects, and environments, or even making new, nonexistent individuals appear real.

As AI gains momentum, greater technological acumen, and societal acceptance, the gap between reality and a technologically created reality will slowly narrow and if not appropriately addressed, eventually disappear.

Table 2.8 Types of Disinformation

DISINFORMATION TYPE	DEFINITION	EXAMPLE
AI hallucinations	When an AI system generates incorrect or nonsensical outputs.	An AI assistant says the moon is made of cheese, even though that's not true.
Biased information	Information presented in a way that unfairly favors one side or viewpoint.	A news article that only shows positive stories about one sports team and ignores their losses.
Clickbait	Sensational or misleading headlines designed to attract attention and clicks.	A headline saying, "You Won't Believe What This Kid Found in His Backyard!" when it's just a rock.
Deepfakes	Videos or audio recordings that have been altered using AI to make it look or sound like someone else.	A video showing a famous athlete saying things they never actually said.
Disinformation	False information spread deliberately to deceive people.	A social media post claiming that raw carrots cure all diseases, which is not true.
Fabricated content	Completely made-up information meant to deceive people.	A false news article claiming a local school is giving out free mobile phones to every student, which never happened.
Fake news	News stories that are not true, created to mislead people.	A headline saying a famous actor moved to your town, which is completely false.
False context of connection	Real information presented with false context to mislead.	A real photo from a movie set shown as if it was a real-life event.
Hoaxes	Deliberate tricks or deception intended to fool people.	A fake news report about a UFO sighting that never happened.
Imposter content	Content made to look like it comes from a real, trusted source, but it's fake.	A fake website that looks like a legitimate news channel but spreads false information.
Malinformation	Information that is true but is spread with the intention to cause harm or manipulate.	Leaking someone's private messages online to embarrass them.
Manipulated content	Information that has been altered or edited to mislead.	A photo of a person digitally edited to show them in a place they've never been.
Misleading content	Information that is technically true but presented in a way that misleads people.	A headline saying, "Local School Cancels All Classes!" when it was just for 1 day due to snow.
Parody	Imitation of something real, made for humor, not to deceive.	A video pretending to be a news report but making jokes about how pets are secretly running the government.
Propaganda	Information spread to promote a particular political cause or point of view, often biased or misleading.	A poster showing only the good things about a candidate while ignoring any bad things.
Rumors	Unverified information spread by word of mouth or online.	A rumor that the school will close for an extra week during the summer, but no one knows for sure if it's true.
Satire	Content meant to be funny and make fun of real events, not to be taken seriously.	A funny article on your school's website, joking that the government is banning all homework because students love it too much.

Malinformation: Information that is based on reality but is used with harmful intent, often by revealing private, sensitive, or true information to deliberately cause harm, manipulate public perception, or damage reputations. It differs from misinformation (false but not intended to harm) and disinformation (deliberately false with intent to mislead).

The ability of advanced technologies, specifically AI, to adversely and easily manipulate data and then present that data as original, unmodified content is worrisome to the highest level.

A 2023 global study conducted by the security firm McAfee, found that out of 7,000 people surveyed, 70% of survey respondents said *they weren't confident* they could tell the difference between a cloned voice and the real thing.

Addressing the impact of that cloned voice, nearly half (45%) of the same survey respondents said they would reply to a voicemail or voice message purporting to be from a friend or loved one in need of money, particularly if they thought the request had come from their partner or spouse (40%), mother (24%), or child (20%).[43]

In one study, "The Spread Of True And False News Online," researchers found that false news spread to more people than true news. The top 1% of false news stories reached between 1,000 and 100,000 people, while true stories rarely reached more than 1,000 people. Additionally, false news spreads more quickly than the truth.[44]

How Are Deepfakes Used?

Table 2.9 provides a list of some of the basic uses of deepfakes by threat actors. It is useful to incorporate information from this table into class discussions and exercises on recognizing deepfakes.

Table 2.9 Deepfake Usage

Disinformation campaigns	Deepfakes are used to spread false information, often for political manipulation or to destabilize trust in public figures or institutions.
Fraud and identity theft	Criminals use deepfakes to mimic someone's appearance or voice to commit financial fraud, trick businesses, or access sensitive information.
Entertainment and media	Deepfakes are increasingly used in films or media to recreate actors, de-age characters, or generate special effects.
Pornography	Nonconsensual deepfake pornography, often involving celebrities or regular individuals, is a harmful and growing misuse of the technology.
Political manipulation	Deepfakes are employed to create fabricated videos of politicians or world leaders, making it appear as though they said or did something they did not.
Corporate espionage	Deepfakes can be used to impersonate CEOs or executives in video conferences, leading to security breaches or manipulation of financial markets.
Scams	Deepfakes are used in phishing attacks or social engineering schemes to impersonate family members, colleagues, or authority figures to extract money or sensitive data.
Journalistic manipulation	Deepfakes can be created to discredit journalists or media outlets by fabricating statements or actions to undermine their credibility.
Creative art and satire	Some use deepfakes for artistic purposes or to create satire, blending real and fictional content for creative expression.
Digital entertainment & video games	Deepfakes are sometimes used to create realistic in-game characters or enhance virtual experiences by personalizing characters to look like real individuals.

Mitigating Deepfake Risks

The following is a list of recommendations that educators can share with students regarding proactive actions that students can take to mitigate the risks of deepfakes.

1. Be Skeptical of What You See and Hear Online: Don't believe everything you see or hear in videos or audio clips. If something seems strange or too extreme, it could be manipulated or fake.
2. Verify Information with Trusted Sources: Before sharing any video or audio clip, check if it's being reported by reliable news sources. Look for information from established and trustworthy websites.
3. Look for Signs of Manipulation: Watch for odd facial movements, unnatural voice tones, or strange video transitions that might indicate a deepfake. If something seems off, it might be fake.
4. Don't Share Content without Thinking: Before forwarding or posting a video or audio, ask yourself if it could harm someone or spread false information. It's better to be cautious than to share something harmful.
5. Use Reverse Image and Video Search Tools: Use tools like Google Reverse Image Search or TinEye, for example, to see if an image or video is real or has been altered. This can help spot fake content early.
6. Protect Your Personal Information: Avoid sharing personal images, videos, or details online that someone could misuse or manipulate. Keep your social media profiles private and only accept friend requests from people you know.
7. Report Fake or Harmful Content: If you come across a deepfake or a video that looks suspicious, report it to a trusted adult, your teacher or school official, or the website where you found it.
8. Discuss with an Adult: If you're unsure whether something is real or fake, talk to a parent, teacher, or another trusted adult. These people you trust can help you figure out what's true and what isn't.
9. Be Cautious with Apps and Filters: Some apps that change faces or voices might seem fun, but they could also collect your data or misuse it. Only use apps with good reviews and always check the privacy and security settings.
10. Build Media Literacy Skills: Keep on learning. Advise your students to learn how deepfakes are made and how to recognize them. The more you know about how the media works, the better students will be at spotting fakes.

These recommendations are designed to encourage students to think critically, protect their privacy, and act when they suspect something may be a deepfake.

Educators, these tips can be discussed with your students and/or included in small-group, in-class exercises. These recommendations and overall discussion on deepfakes, fake news, etc., may be incorporated into a broader media literacy program designed to assist students in navigating safely in today's digitally dependent society.

What Is Media Literacy?

Media literacy involves critically evaluating online content, distinguishing between reliable sources and misinformation, and understanding the impact of fake news.

It involves understanding the role media plays in society, recognizing its messages, identifying bias, and distinguishing between credible information and misinformation. This skill empowers individuals to critically engage with media, make informed decisions, and responsibly produce content. Media literacy helps foster critical thinking and promotes informed participation in our increasingly digital, media-rich world.

Seventh and eighth-grade students should understand the basics of media and information literacy. Doing so will equip them with the critical thinking skills needed to live and interact in their technically rich digital environment.

This knowledge helps students to identify credible sources, distinguish between fact, fake news, and misinformation, and evaluate the intent (actual and implied) behind various social media/networking messages. In today's 24/7 digitally connected society, students are constantly exposed to online information; therefore, media literacy skills are essential for making informed decisions, fostering responsible online behavior, and preparing students for future academic and personal challenges.

The National Association for Media Literacy Education (NAMLE) offers the following definitions when defining media literacy:

- Media refers to all electronic or digital means and print or artistic visuals used to transmit messages. Literacy is the ability to encode and decode symbols and to synthesize and analyze messages.
- Media literacy is the ability to encode and decode the symbols transmitted via media and synthesize, analyze, and produce mediated messages.
- Media education is the study of media, including "hands-on" experiences and media production.
- Media literacy education is the educational field dedicated to teaching the skills associated with media literacy.[45]

The impact of generative AI (e.g., ChatGPT, Claude, etc.) will have a significant impact on our global digital society. The speed, capability, and ease with which AI can create and disseminate manipulated and false content is easier to create and harder to identify.

With the proliferation of misinformation online, students need to develop critical thinking skills. Media literacy helps students navigate the Internet more safely and ensures they are informed and discerning consumers of digital content.

Reaching and Teaching Students about Media/Information Literacy

Teaching Tip

The following is a five-step approach that educators may use to teach media/information literacy to 7th and 8th-grade students.

Step 1: Introduction to Media Types

Objective: Help students identify different forms of media (social media, news, blogs, etc.) and understand how each type shapes information.

Step 2: Understanding Bias

Objective: Teach students how to recognize bias in media sources and differentiate between opinion and fact-based reporting.

Step 3: Evaluating Credibility

Objective: Guide students in assessing the credibility of sources using critical questions like "Who created this content?" and "What is their intent?" AI techniques such as machine learning and deep learning are being leveraged to deceive people by creating and disseminating fake content.

Step 4: Fact-Checking Tools

Objective: Introduce fact-checking websites and tools (e.g., Snopes, FactCheck.org, TinEye, etc.) that students may use to verify information.

Step 5: Responsible Sharing

Objective: Promote responsible online behavior, teaching students how to avoid spreading misinformation and encouraging thoughtful, informed discussions.

The greatest defense against fake news, misinformation, disinformation, and malinformation, is educating students and arming them with facts. Students who endeavor to seek out diverse, verifiable sources of information and think critically before naively believing or sharing information online will significantly reduce the reach and impact of those who create and purvey fake news and all of its related cousins.

The Impact of Screen Time

This topic, equally important to students, explores the effects of excessive screen time on physical and mental health, including its impact on sleep, attention, and social interactions. Educators should discuss this topic with students as students need to be made aware of the potential mental, physical, emotional, and psychological effects of prolonged screen time.

Excessive screen time can lead to negative health outcomes. Educating students about balanced screen use encourages healthier habits, helping them manage their time (a skill that they will need both as they continue their academic journey and also when they enter the workforce) and maintain a healthy lifestyle in a technology-driven world.

Defining Screen Time

"Screen use" or screen time among tweens (8–12 years) or teens (13–18 years) typically refers to time spent interacting with digital media devices such as smartphones, tablets, computers, televisions, video gaming, watching videos, and participating in social media activities such as texting, video chatting, browsing the Internet, etc.

Studies have shown that the pandemic led to increased screen use for social interaction, entertainment, and leisure, especially as many individuals spent more time at home during lockdowns.

This measure of screen use generally excludes time spent on educational activities and focuses on recreational or social engagement through screens during nonschool hours. See Figure 2.7 for a quick overview of screen time usage by tweens and teens.

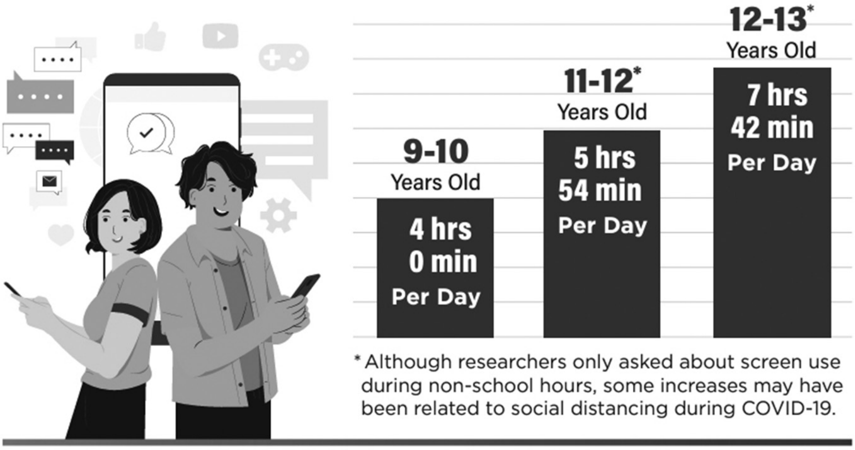


Figure 2.7 Youth use screens more as they get older.[46]

Excessive screen time has become a common global behavior among children and adolescents.

According to research reviewed by Qi et al., "Screen Time Among School-Aged Children of Aged 6–14: A Systematic Review," the average screen time of school children aged 6–14 was 2.77 hours per day, and 46.4% of them had an average screen time of ≥2 hours per day. The average rates of school-aged children who had screen time within the range of ≥2 hours per day were 41.3% and 59.4%, respectively, before and after January 2020.[47]

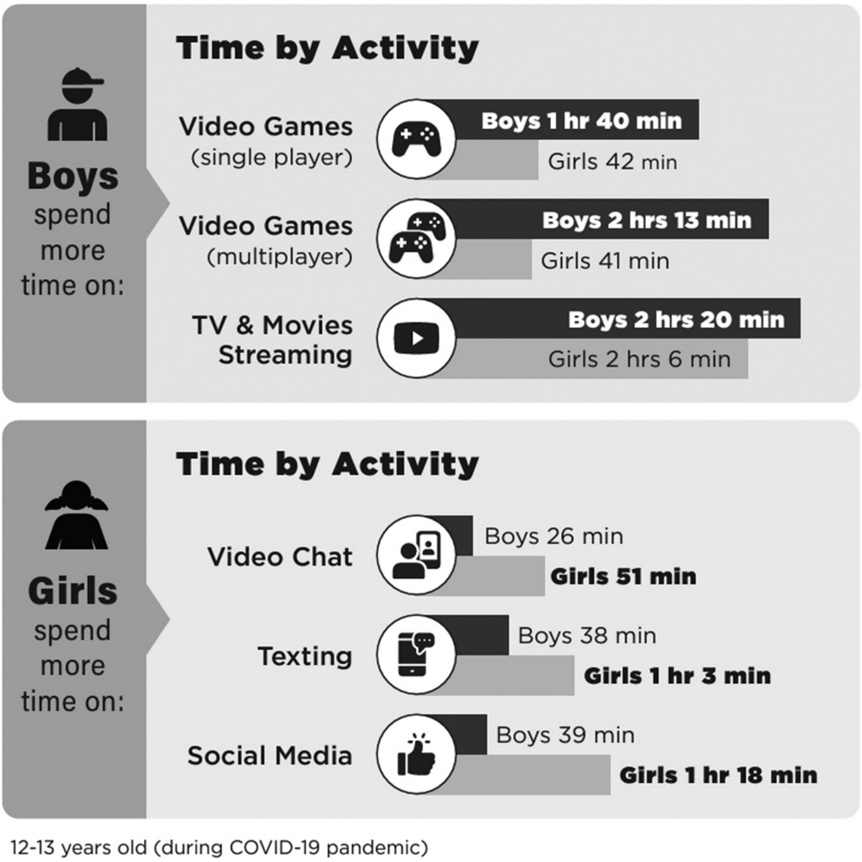


Figure 2.8 Average daily screen use by gender.[48]

Figure 2.8 provides a glimpse at screen time activities by gender from a study conducted by the National Institutes of Health in 2024.

Exploding Topics reported that for American teens (13- to 18-year-olds), screen time has increased by 29.75% since 2015.

According to the latest available data, teenagers spend **7 hours and 22 minutes per day** in front of screens.

That equates to 43% of a teen's waking hours. By comparison, that's 24 minutes more than the global average of 6 hours 58 minutes.

Screen time continues to increase across the population, but it's perhaps most alarming in teenagers. At well over 7 hours, many teens are spending almost half of their waking hours looking at screens … a concerning statistic (see Figure 2.9).

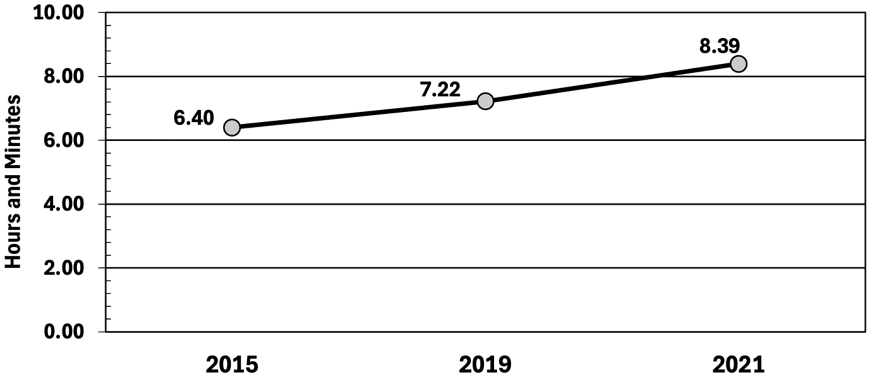


Figure 2.9 Average daily screen time. American teens (13- to 18-year-olds).[49]

That means that since 2015, average screen time among teens has increased by 1 hour and 59 minutes!

How Much Time Is Too Much?

While current research and available evidence do not establish a direct causal link between digital media use and negative mental health outcomes like depression and anxiety, it is still prudent for tweens and teens to act proactively in managing their screen time and for educators, parents, caregivers, and trusted adults, to discuss possibly the potential for overuse of screen time with students.

Excessive screen time can potentially lead to issues such as reduced physical activity, disrupted sleep patterns, and reduced face-to-face social interactions, all of which can contribute to an individual's overall well-being. By discussing these potential exposures and establishing healthy usage parameters, students are in better control to monitor that screen time does not interfere with other equally important aspects of their lives.

Additionally, disproportionate screen use, particularly on social media, has been linked to potential emotional risks such as increased exposure to cyberbullying, unhealthy comparisons, and the pressure to constantly stay connected.

The United Kingdom's Office of Communications (Ofcom) reporting in 2023 on the downsides of being online showed that individuals aged 8–17 identified with the negative aspects of using social media or messaging apps or sites: Two-fifths of 8–17-year-olds thought that people were mean or unkind to each other on social media and messaging apps or sites all or most of the time, while 26% believed there was pressure to be popular on these types of platforms all or most of the time (see Figure 2.10).

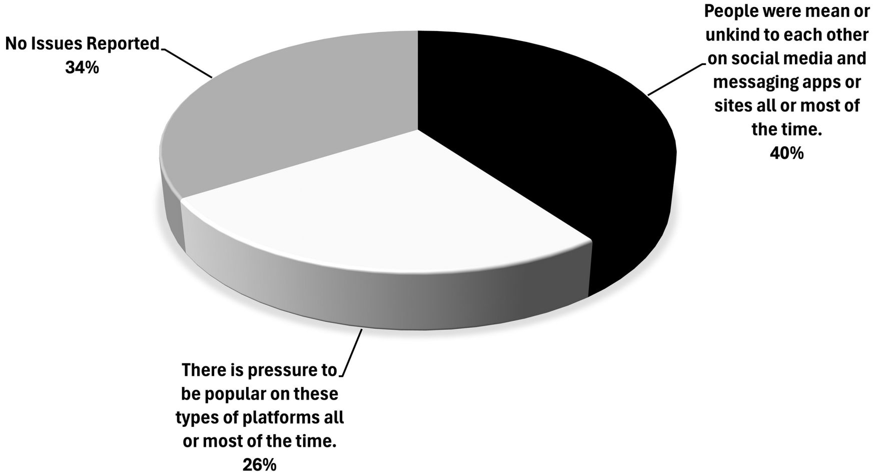


Figure 2.10 Downside of being online.[50]

BK 4 CHPT 2 — Lesson Plans Section Divider Graphic

Being proactive in monitoring screen time helps avoid these pitfalls, allowing tweens and teens to maintain a balanced perspective and healthier self-esteem, realizing that over time, using digital devices and screen time for meaningful, engaged learning rather than passive consumption may help to reduce the risks associated with stress and mental fatigue.

Developing positive habits toward an evenhanded approach to screen time utilization prepares young individuals with the skills they need for self-regulation, a critical component of mental resilience. Learning how to manage screen time effectively, along with prioritizing offline activities such as exercise, hobbies, and personal relationships, helps to create a balanced lifestyle that can protect against the potential negative impacts of excessive digital engagement.

Recommendations for Monitoring and Managing "Screen Time"

The following recommendations should be reviewed by parents, caregivers, and educators when discussing approaches to promoting a healthier balance between screen time usage and off-screen activities.

1. Set Time Limits for Screen Use: Establish clear rules around daily screen time that encourage tweens/teens to engage in offline activities, such as hobbies, sports, or family time. Use parental control apps if necessary to help with time management.
2. Encourage Physical Activities: Promote outdoor play, exercise, and sports, which naturally reduce the desire for screen time while contributing to physical and mental health.

3. Model Positive Screen Habits: Adults should lead by example by reducing their own screen time during family meals, outings, or before bed. This helps reinforce healthy behavior patterns for everyone.
4. Promote Offline Hobbies: Encourage tween/teens to develop interests outside of the digital world, such as reading, drawing, music, or crafts. This will provide them with fulfilling alternatives to screen use.
5. Designate "Screen-Free" Zones: Parents, implement screen-free times or areas in the house, such as during meals, in bedrooms, or an hour before bed. These boundaries help to reduce screen time naturally.
6. Educate on Digital Well-Being: Educators, teach students about the potential effects of too much screen time on their eyes, sleep, and mental health. Make them aware of the importance of balanced digital consumption.
7. Use Screen Time Productively: Educators and parents, emphasize using screens for educational purposes or creative activities rather than solely for entertainment. This way, screen time is more meaningful and less likely to be wasted.
8. Engage in Family Activities: Parents, plan regular family activities that do not involve screens, such as board games, cooking, or outdoor adventures, fostering stronger bonds and reducing reliance on digital entertainment.
9. Track and Reflect on Screen Time: Parents and educators, help tweens/teens monitor their screen usage using apps or journals. Encourage them to reflect on how they feel after long screen sessions vs. engaging in other activities, helping them self-regulate.
10. Create a Reward System for Reduced Screen Time: Educators and parents offer incentives or rewards when screen time limits are achieved or when engaging in alternative activities. This positive reinforcement encourages long-term healthy habits.

We must be careful not to focus so narrowly on protecting our youth in the real world while leaving them vulnerable in the digital world!

Ethical Use of Technology

Simply stated, the effective and ethical user of technology is the ability to use a variety of technologies effectively and ethically.

Under this topic, educators discuss and teach, and students learn about the ethical implications of their digital actions, including respect for intellectual property, avoiding plagiarism, and using technology for positive purposes.

Understanding the ethical use of technology fosters responsible behavior online. This topic is essential for helping students respect others' work, avoid legal issues, and contribute positively to the digital community.

The reader is directed to Chapter 1 where the ethical use of technology including recommendations for discussing this topic with students has been addressed extensively.

Risks of Digital Social Networking: Inappropriate Content

The Internet has brought advantages such as access to information and friends anywhere in the world and at any time, but it can also contain information, images, videos, and even virtual spaces that are inappropriate or not age-appropriate for students.

Adolescents and children can unintentionally come into contact with inappropriate content online, such as sexually explicit material, or can stumble across adult-only online spaces, such as adult-only virtual worlds. Unsolicited, obscene materials can also be received electronically.

Adults in the school community need to help students learn how to be good digital citizens and navigate online spaces safely to avoid coming into contact with or disseminating inappropriate content.[51]

Educators teaching students to be vigilant and cyber-safe must plan discussions and class exercises designed to remind students that if they come across anything harmful or inappropriate, or content or websites that make them feel uncomfortable, report it to a teacher, a trusted adult, or if available to the site administration where the content was found. Just like telling a teacher about bullying at school, students need continual reinforcement to report harmful online behavior to keep everyone safe.

Reviewing the following topics, while sensitive and at times challenging to discuss with students, will provide your students with the knowledge to better protect themselves and to be proactive, vigilant, and cyber-safe while working, living, and playing online and offline.

The following topics that address risks and inappropriate online content are not exhaustive, as such a list or discussion may never be, in a continually evolving digital environment. These topics are, however, critical issues! Educators teaching students to be cyber-safe in a digital world must engage in frank, open, fact-based, and honest discussions with students.

The information that follows is presented to both broaden the reader's awareness and understanding of these critical topics and to provide the reader with recommendations on starting the discussion.

Sexting and Sextortion

Sexting is the sharing and receiving of inappropriate content in the form of sexually explicit messages, photos, or videos via text messages or apps. Sexting, while commonly occurring off school grounds, is increasingly occurring on school property, with content being sent and viewed on cell phones.

Research released in 2020 disclosed that approximately 5% of students reported that they had been the victim of sextortion, while about 3% admitted to threatening others who had shared an image with them in confidence.[52]

In discussing this important topic and its relevance to staying cyber-safe, it is critically important to make sure that students fully understand that the possession of sexually explicit photos received by sexting may have serious legal consequences as it can be considered a type of possession of child pornography.

Sexting may also be used to pressure someone into having sex or to extort money or sex from a victim ("sextortion"). US state laws on sexting vary widely, from decriminalization to misdemeanor charges or prosecution for child pornography with harsh sentences. Teen behavior and digital invention have outpaced the development of new laws, and this has the potential to have dire legal ramifications for teens.[53]

Sextortion should be distinguished from revenge porn, known less colloquially as "nonconsensual pornography," another behavior involving the unauthorized distribution of explicit images. The primary difference between the two is that revenge porn tends to be public while sextortion is usually private (unless threats are ultimately carried out). With revenge porn, the aggressor is seeking to publicly humiliate the target, whereas with sextortion the aggressor is attempting to privately extort something of value from the target.[54]

US Federal Law Section 2251 of Title 18, United States Code, makes it illegal to persuade, induce, entice, or coerce a minor to engage in sexually explicit conduct for purposes of producing visual depictions of that conduct. Any individual who attempts or conspires to commit a child pornography offense is also subject to prosecution under federal law.

Any violation of federal child pornography law is a serious crime, and convicted offenders face severe statutory penalties. For example, a first-time offender convicted of producing child pornography under 18 U.S.C. §2251, faces fines and a statutory minimum of 15–30 years maximum in prison.[55]

Global Legislative Overwatch: Sexting and the Law

The United States is not alone in the effort to criminalize and penalize those individuals who engage in sharing or distributing nonconsensual images. The following is a representative sample of countries that have laws that can be applied to sexting, particularly involving minors or nonconsensual sharing.

- Canada: The Criminal Code Section 162.1(1) includes provisions against child pornography and distributing intimate images without consent (this includes text, audio, and video). Penalties for distributing nonconsensual images (Part V of the Criminal Code relating to "Sexual Offences, Public Morals, and Disorderly Conduct") can include imprisonment for up to 5 years.

  Section 162.1 (1) states … Everyone who knowingly publishes, distributes, transmits, sells, makes available, or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct or being reckless as to whether or not that person gave their consent to that conduct, is guilty:

  a. Of an indictable offense and liable to imprisonment for a term of not more than 5 years, or
  b. Of an offense punishable by summary conviction.[56]
- France: The Penal Code (Code penal), Article 227-23, Act no. 2004-204 of 9 March 2004 article 6 VII Official Journal of 10 March 2004, prohibits the dissemination of intimate images without consent, especially regarding minors.
  a. Taking, recording, or transmitting a picture or representation of a minor to circulate it, where that image or representation has a pornographic character, is punished by 3 years imprisonment and a fine of €45,000. Attempting to do so is subject to the same penalties.
  b. The same penalty applies to offering or distributing such a picture or representation by any means, and to importing or exporting it, or causing it to be imported or exported.[57]
- Germany: The German Criminal Code, Special Part – Chapter Thirteen, Section 184b – Distribution, acquisition, and possession of child pornography, criminalizes the distribution of child pornography and includes provisions against the dissemination of personal intimate images without consent.
  a. Whosoever disseminates; publicly displays, presents, or otherwise makes accessible; or produces, obtains, supplies, stocks, offers, announces, commends, or undertakes to import or export to use them or copies made from them shall be liable to imprisonment from 3 months to 5 years.[58]
- India: The Information Technology Act, 2000, Chapter XI, Section 66E, includes provisions against the sharing of sexually explicit material without consent, particularly concerning minors.
  a. Whoever, intentionally or knowingly captures, publishes, or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to 3 years, or with a fine not exceeding 200,000 rupees, or with both.[59]
- New Zealand: The Films, Videos, and Publications Classification Act 1993 addresses the sharing of harmful digital communications, including sexting incidents. A publication is objectionable if it describes, depicts, expresses, or otherwise deals with matters such as sex, horror, crime, cruelty, or violence in such a manner that the availability of the publication is likely to be injurious to the public good. A publication deals with a matter such as sex if:
  a. The publication is or contains one or more visual images of one or more children or young persons who are nude or partially nude.
  b. Those one or more visual images are, alone, or together with any other contents of the publication, reasonably capable of being regarded as sexual in nature.

  c. The use of violence or coercion to compel any person to participate in, or submit to, sexual conduct.
  d. Sexual conduct with or by children, young persons, or both.[60]
- South Africa: Films and Publications Amendment Act, 2009, Chapter 6, Section 24A, paragraph 4, regulates the distribution of explicit content, including child pornography.
  a. Any person who knowingly distributes or exhibits any film, game, or publication classified —— X18 (X-rate 18 years) or which contains depictions, descriptions, or scenes of sexual conduct to a person under the age of 18 years shall be guilty of an offense and liable, upon conviction, to a fine or imprisonment for a period not exceeding 5 years or to both a fine and such imprisonment.[61]
- Singapore: The Protection from Harassment Act 2014, PART II, Article 4, Harassment, alarm or distress, paragraph 1, No person shall by any means
  a. use any threatening, abusive, or insulting words or behavior; or
  b. make any threatening, abusive, or insulting communication, which is heard, seen, or otherwise perceived by any person (referred to in this section as the victim) likely to cause harassment, alarm, or distress.

     Illustrations:
     - Y repeatedly circulates revealing photographs of a classmate (X) to other classmates.
     - X and Y are classmates. X posts a vulgar tirade against Y on a website accessible to all of their classmates. One of Y's classmates shows the message on the website to Y, and Y is distressed. X is guilty of an offense under this section.[62]
- United Kingdom of Great Britain and Northern Ireland: The sharing of sexual images of minors is criminalized. Several legislative acts address this issue in the United Kingdom, Ireland, Scotland, and Wales, specifically, but not limited to
  - Coroners and Justice Act 2009, Section 62(1);
  - Criminal Justice Act 1988, Section 160;
  - Criminal Justice and Immigration Act 2008, Section 63;
  - Protection of Children Act 1978, Section 1[63]; and
  - Sexual Offences Act 2003, Part 1, Chapter 42, Section 15.

Approaching the subject requires sensitivity, along with frank and open conversations. However, being cyber-safe requires being proactive in avoiding activities that will put you at risk. Teaching students to be cyber-safe sometimes requires discussing sensitive subjects.

Sexting: Students at Risk

Educators must continually stress the inappropriateness and dangers of engaging in sexting, with students. This activity exposes them to possible significant and long-term consequences, such as humiliation, extortion, victimization, school sanctions, reputational damage, and even criminal charges.

Educators, do your students know this? Understand this?

Teaching Tip

If someone sends them a sext, they DO NOT share it or show it to anyone else. Sharing such images without consent can be illegal, and as discussed there are strict laws that protect against this kind of behavior. Again, these laws carry serious consequences, especially if the image involves a minor, so it's important to understand that they could face legal trouble by forwarding or showing these images.

Extreme, inappropriate, and harmful content continues to be easily and widely accessible to children and adolescents. This can be spread through direct pushes, unwanted content exchanges, and algorithmic designs. In certain tragic cases, childhood deaths have been linked to suicide- and self-harm-related content and risk-taking challenges on social media platforms.

Offenders often manipulate victims into providing sexually explicit images or meeting the offender's monetary or sexual demands by threatening to post the victim's images online or to share the images with the victim's friends and family. Victims of sextortion may share images or information with someone they believe to be a trusted individual, but in many cases, they are targeted intentionally by someone they met online who may coerce or deceive them into sharing images or information.

Although sextortion occurs online and often (but, not exclusively) outside of school hours, it can have resounding negative impacts on many aspects of the victim's life, including their school life. Sextortion victims have reported experiencing depression, anxiety, hopelessness, fear, and other negative mental health impacts; have dropped out of school at higher rates; and have engaged in self-harm, including threatening, attempting, or committing suicide, at higher rates.

Sextortion can involve other types of cyber threats, including ransomware. Ransomware is a particular form of computer malware in which perpetrators encrypt users' files and then demand payment of a ransom for users to regain access to their data. Ransomware can include an element of extortion, in which the perpetrator threatens to publish data or images, including sexually explicit images, if the victim does not do what the perpetrator wants, such as provide nude photos.[64]

It is also important to note from previous discussions that social media platforms can be sites for predatory behaviors and interactions with malicious actors who target children and adolescents.

Online Enticement

Online enticement occurs when an individual communicates online with a child with the intent to commit a sexual offense or abduction. Online enticement can happen on instant messaging, social media, online gaming platforms, or in other online spaces. Online predators may engage in grooming, by which they build the victim's trust by developing a rapport, sympathizing with him or her, engaging with online posts, or feigning common interests.[65]

Grooming and online enticement can lead to child sexual exploitation, sextortion, and adult sexual misconduct (ASM). The US Government Accountability Office defines ASM as any sexual activity directed to a child to develop a romantic or sexual relationship. Behaviors may range from those that are inappropriate to those that are illegal, and they may include verbal conduct, physical conduct, or electronic interactions. ASM can be perpetrated by educators but also by other school personnel, including athletic coaches, administrative staff, bus drivers, or volunteers.[66]

Topics for Classroom Discussion

The Internet provides a wealth of opportunities, including access to vast information and global connections, but it also presents risks, especially for adolescents who may encounter inappropriate content or harmful interactions online.

Sexting, the exchange of sexually explicit messages or images, has become increasingly common among young people, with serious legal, emotional, and social consequences. Educators must engage in open, fact-based discussions with students about the dangers of sexting and the severe legal ramifications, such as potential charges related to child pornography, which could have lifelong implications.

Educators must emphasize the importance of cyber safety and the need for students to report inappropriate or threatening behavior to trusted adults. These conversations, while they may be difficult or stressful to initiate and have, are essential to assisting students understand the dangers of sexting, remain vigilant online, and protect themselves from becoming victims of online exploitation.

Ultimately, educators, parents, and caregivers play a vital role in equipping students with the knowledge and tools to navigate the digital world safely.

The reader is directed to Chapter 3, where these topics are discussed further.

Digital Literacy

To refresh from Chapter 1, most teachers wish students spent less time on social media, and most students are tired of being reminded how bad social media is all the time. Instead of focusing on the negative, teach students how to use social media responsibly through media literacy. That means teaching students explicitly how digital media demands attention and how to make smart choices about what they read, watch, and listen to online.

It is understood that media literacy is the practical, cognitive, and affective competencies required to access, analyze, evaluate, and create content on social media in a variety of contexts. Therefore, the concept of social media literacy is based on media literacy to then integrate the characteristics and the implications of digital platforms.[67]

Digital literacy requires students to not only comprehend a digital text but also learn how to navigate online spaces. Digital content typically includes hyperlinks, videos, audio clips, images, and comments. Combining these extra elements requires the reader to stop and make decisions instead of just reading from top to bottom. While these elements create a complex intertextual web of diverse content, learning how to navigate between them is essential for their futures.[68]

The reader is directed to Chapter 1 where the topic of digital literacy is addressed in greater depth.

Basic Cybersecurity Awareness

A discussion with students on this topic involves understanding common cybersecurity threats like viruses, malware, and hacking, and learning basic protective measures such as antivirus software and safe browsing habits.

Basic cybersecurity knowledge is essential as students increasingly use the Internet. Knowing how to protect their devices and data from cyber threats ensures a safer online experience and prepares them for more complex cybersecurity challenges in the future.

Research conducted by the Office of Communications in the United Kingdom showed that nine in ten 8–17-year-olds (91%) had talked to someone about how to use the Internet safely, and of those who had, 88% had done so with any family member, usually a parent (86%). Similarly, 80% had received information about how to use the Internet safely from someone outside the family, most commonly a teacher (76%).[69]

When cybersecurity is inadequate, it can lead to stolen identities and financial loss. Most scams and scammers have two main goals: to steal money and identities. Your discussions with students should focus on what to look for, how scammers and threat actors operate, and what to do, so they can protect themselves both in their online digital world and offline.

Maintaining cybersecurity is very important, even for students. It is not simply something that concerns large corporations and other businesses.

The topic of cybersecurity is broad and encompassing. A topic whose full coverage is well beyond the scope of this book. The following cybersecurity concern presents a threat to everyone's safe cyber activities. Due to the timeliness of the topic, it has been included here.

Scattered Spider and The Com

Scattered Spider, (a.k.a. UNC3944), is a cybercriminal group known for sophisticated phishing attacks and social engineering tactics. They target major corporations and infrastructure by tricking employees into revealing login credentials, which are then used for breaches and data theft.

The Com is another criminal group, often associated with ransomware attacks, and is known for compromising organizations through malware, encrypting data, and demanding ransom for its release.

Educating middle school students about Scattered Spider and The Com is important because these groups use techniques like phishing and social engineering, which can target anyone, adults and kids alike. Understanding these threats helps students recognize malicious online behavior, keep personal information secure, and avoid falling victim to scams.

Basic Cybersecurity Awareness Recommendations

1. Never Share Personal Information: Advise students to secure their personal information. Students should never provide passwords, home addresses, or personal details to anyone online unless verified. Before providing any personal information, such as their date of birth, Social Security number, account numbers, and passwords, online, be sure the website is secure.
2. Be Skeptical of Emails and Messages: Phishing emails may look legitimate but contain subtle clues that they are fake. Teach students to avoid clicking on suspicious links or attachments. Do not open emails from people they don't know. If they are unsure whether an email received is legitimate, advise them to try contacting the sender directly via other means. Do not click on any links in an email unless they are sure it is safe.
3. Use Strong, Unique Passwords: Passwords should be hard to guess and not reused across multiple accounts.
4. Enable 2FA: Encourage the use of 2FA for all important accounts, adding an extra layer of security.
5. Keep Software Updated: Make sure students know to keep their apps and devices updated to protect against malware. Discuss with students the importance of installing software that provides antivirus, firewall, and email filter services.
6. Update the OSs on All Electronic Devices: Make sure that students routinely check for updates to OSs and applications to ensure that they are up to date on all of their electronic devices. Older and unpatched versions of OSs and software are the target of many hacks.
7. Stay Informed on the Latest Cyber Threats: Teach students to keep up to date on current scams. The CISA (www.cisa.gov) can provide students with alerts and help them stay alert to current scams.
8. Be Careful with Links and New Website Addresses: Malicious website addresses may appear almost identical to legitimate sites. Scammers often use a slight variation in spelling or logo to lure you. Malicious links can also come from friends whose email has unknowingly been compromised, so be careful.

9. Report Suspicious Activity: Encourage students to tell a trusted adult, a teacher, or a caregiver if they receive suspicious messages or emails that seem unusual or threatening.

For educators seeking to keep abreast of the ever-evolving world of cybersecurity and the global effects of cybersecurity events, Table 2.10 provides a list of organizations

Table 2.10 Cybersecurity — Global Information Resources

ORGANIZATION NAME AND WEBSITE	CYBERSECURITY INFORMATION PROVIDED
Center for Internet Security (CIS) www.cisecurity.org	Provides best practices, tools, and resources to protect against cybersecurity threats, including the CIS controls and CIS benchmarks.
Cybersecurity and Infrastructure Security Agency (CISA) www.cisa.gov	US governmental agency offering resources on cybersecurity, infrastructure resilience, alerts, and vulnerability management.
European Union Agency for Cybersecurity (ENISA) www.enisa.europa.eu	Publishes cybersecurity strategies, threat landscape reports, and security guidelines for the EU and globally.
Global Forum on Cyber Expertise (GFCE) www.thegfce.org	A platform for global cybersecurity capacity building, sharing expertise, best practices, and resources to improve cybersecurity worldwide.
Internet Society (ISOC) www.internetsociety.org	Provides information on Internet security, privacy, and Internet governance, with a focus on building a safer, more secure Internet.
Interpol Cybercrime Unit www.interpol.int	Coordinates global efforts to combat cybercrime and disseminates information about emerging cyber threats and law enforcement collaboration.
International Telecommunication Union (ITU) www.itu.int	A specialized UN agency that provides global guidelines and reports on cybersecurity standards, cooperation, and development strategies.
MITRE corporation www.mitre.org/focus-areas	Manages the Common Vulnerabilities and Exposures system and publishes cybersecurity frameworks like ATT&CK for threat modeling and mitigation.
National Cyber Security Centre (NCSC — UK) www.ncsc.gov.uk	Provides cybersecurity guidance, threat intelligence, and response services for UK citizens, businesses, and government organizations.
National Institute of Standards and Technology (NIST) www.nist.gov/cybersecurity	US agency that develops cybersecurity standards, guidelines, and frameworks (e.g., NIST Cybersecurity Framework) for protecting critical systems.
Open Web Application Security Project (OWASP) www.owasp.org	Offers free resources on software security, including the widely known OWASP top 10 vulnerabilities, tools, and methodologies.
SANS Institute www.sans.org	Provides cybersecurity training, research, certifications, and threat intelligence resources for professionals globally.
Software Engineering Institute CERT Division Cybersecurity Center Development www.sei.cmu.edu/our-work/cybersecurity-center-development/index.cfm	Partners with government, industry, law enforcement, and academia to improve the security and resilience of computer systems and networks and develops advanced methods and tools to counter large-scale, sophisticated cyber threats.
World Economic Forum (WEF) Cybersecurity Center https://centres.weforum.org/centre-for-cybersecurity/home	Shares insights on global cyber risks, best practices, and initiatives for public–private cooperation on cybersecurity.
Center for Internet Security (CIS) www.cisecurity.org/controls	Provides best practices, tools, and resources to protect against cybersecurity threats, including the CIS Controls and CIS Benchmarks.

that disseminate daily (sometimes more frequently) updates on all things cybersecurity-related. Students may also find the information provided by these organizations insightful, relevant, and interesting.

The topic of cyber safety is addressed extensively throughout the four chapters of this book.

Emerging Technologies — A Look Ahead

When simply defined, particularly within the context of education, emerging technologies are those that have the potential to change the current state of affairs in education. Change is at the core of these technologies, both because they evolve and also arguably because their raison d'être is to transform the learners' current experience.[70]

There have been many authors researching and writing on the topic of emerging technologies for teaching and learning. Given the increasingly rapid growth and impact of these technologies, incorporating class discussions and assigned work on the topic of emerging technologies is no longer an option but a necessity.

When reading the literature on both the IT industry and academic sources, the overlap in identifying exactly what emerging technologies are for teaching and learning is considerable.

Though beyond the scope of this book, the following list of topics should be considered as important learning concepts for students entering the mid-21st Century. Each of these areas will have a profound effect on the lives of these students and their children and their children's children. Acquiring fundamental knowledge on these topics will enable students to grow to become savvy, responsible digital citizens who can navigate the online world safely and thoughtfully.

The list of these technologies is in constant flux, as one can only imagine. As of this book's publication date, the most agreed-upon list identifying emerging technologies for teaching and learning are as follows:

- Artificial Intelligence*
- Augmented Reality
- Blockchain
- Cloud Computing
- Internet of Things
- Machine Learning*
- Natural Language Processing*
- Robotics
- Speech Recognition
- Virtual Reality

*Topics addressed in this book.

Summary

This chapter addresses the critical responsibility of equipping seventh and eighth graders with the skills to navigate an increasingly digital world. As these students grow more independent online, the potential risks they face — such as cyberbullying, privacy breaches, and exposure to inappropriate content — become more significant. The chapter emphasizes the importance of transitioning from simply monitoring students' online behavior to teaching them how to identify and manage online and digital risks, ultimately fostering responsible digital citizenship.

The chapter outlines key cyber safety topics for educators to incorporate into lessons, including online privacy, social media best practices, digital footprints, and cybersecurity basics. Through engaging discussions and assignments, educators can empower students to recognize and mitigate online threats, such as phishing scams and cyberbullying. By discussing these issues and integrating them into school curricula, educators can guide students toward safer and more informed online behavior, preparing them for the evolving challenges of the digital world.

LESSON PLANS

Grade 7

TOC Title: G7 Digital Citizenship

Lesson Title: Digital Citizenship
Grade Level: 7
Duration: 45 minutes without video

Objective:

- The students will be able to define digital citizenship and explain its importance.
- The students will understand the concept of a digital footprint.
- The students will understand and practice respectful communication in online spaces.

Suggested Materials:

- Whiteboard or chart paper.
- Markers.
- Printed digital citizenship scenarios (provided below)
- Video such as Being a Good Digital Citizen — YouTube, or another age-appropriate video covering how to be a good digital citizen (3 minutes 42 seconds), or a similar age-appropriate video.

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask students what they think it means to be a good citizen online. Write some of their answers on the board.
b. Define Digital Citizenship — using the Internet responsibly and safely. Discuss the key points of digital citizenship:
    i. Safety: Keeping personal information private.
    ii. Respect: Treating others kindly online.
    iii. Responsibility: Thinking before you post or share information.
    iv. Ask students why being a good digital citizen is important.

Lesson (15 minutes):

a. **Digital Footprint (5 minutes)**:
    i. Explain that everything we do online leaves a trace, called a digital footprint.
    ii. Ask students to give examples of things that could be part of their footprint (posts, photos, comments).

    iii. Draw a simple footprint on the board and label examples inside it to make it visual.

b. **Internet Safety Tips (5 minutes)**: Discuss the following safety tips:
    i. Do not share personal information (like full name, address, or school name).
    ii. Avoid talking to strangers online.
    iii. Use strong passwords and do not share them.
    iv. Write the tips on the board as you discuss.

c. **Respectful Communication (5 minutes)**:
    i. Emphasize the importance of being kind and respectful online.
    ii. Ask students to give examples of kind vs. unkind online behavior.

Digital Citizenship Scenarios (15 minutes):

a. Split the class into small groups (three to four– students per group).
b. Give each group a Digital Citizenship Scenario.
c. Each group discusses the best solution to their scenario for 3–5 minutes.
d. After discussion, each group shares their scenario and solution with the class.
e. As a class, evaluate each solution and discuss if anything else could have been done.

Conclusion (5 minutes):

Summarize the lesson's key points:

a. Stay safe online by protecting your personal information.
b. Be respectful to others in digital spaces.
c. Think before you post because everything leaves a digital footprint.

Assessment:

a. An informal assessment can be taken based on student participation in discussions and activities.

Scenarios for Group Activity:

Scenario 1: You see a post online that makes fun of someone in your class. The post has a lot of likes and comments. What should you do?

Scenario 2: You receive a message from someone you do not know. They want to know where you live and ask for your phone number. What should you do?

Scenario 3: You took a photo at a school event and want to post it online, but the picture includes your classmates. What should you consider before posting?

Scenario 4: You find an interesting article online and want to share it, but you think that it may not be true. What should you do before sharing it?

Scenario 5: You have created a strong password, but one of your friends keeps asking for it. They say it is a good idea in case forget it. What should you do?

Scenario 6: You notice that someone in an online group chat is being left out of the conversation on purpose. Some people are ignoring their messages or responding rudely. What should you do?

Scenario 7: A friend sends you a link to a funny video, but when you click on it, it takes you to a website that looks strange. What should you do next?

Scenario 8: You want to download a new game, but before downloading, the app asks for access to your camera, location, and contacts. What should you consider before agreeing?

TOC Title: G7 Cyber safety
Lesson Title: Cyber safety
Grade Level: 7
Duration: 40 minutes

Objective:

- The students will understand the importance of online privacy.
- The students will know and be able to recognize potential online dangers.
- The students will be able to protect themselves from cyberbullying, harmful content, and online scams.

Suggested Materials:

- Whiteboard, chalkboard, or chart paper.
- Markers.
- Printed or posted scenario for online privacy discussion.
- Printed or digital examples of scams/dangerous content (provided below)

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask students how much time they spend online every day. Ask what cyber safety means and why it is important.
b. Ensure students understand:
    - The Internet is a tool for learning, socializing, and entertainment.
    - Dangers exist online, just like in the real world.
    - The importance of protecting personal information.

Online Privacy Scenario (10 minutes):

a. Share the following scenario with the class: Sarah, a seventh grader, just joined a popular social media platform. She has posted pictures from her birthday party, including a selfie in front of her house with the street sign visible. In the post, she writes, "Just had the best birthday party ever at home! Thanks, everyone! I can't wait to go to Mario's next Friday night at 7 p.m. for the best pizza in the world! Come join me if you're free!"
b. Questions for group discussion:
    - What personal information has Sarah shared that could put her at risk?
        i. Possible responses: Anyone who sees the post can figure out where she lives, when her birthday is, what she looks like, where her favorite pizza place is, and when she will be there.
    - What are the possible consequences of sharing details like her location, birthday, and plans online?

    i. Possible response: Unsafe people can use this information to find Sarah.
- What could Sarah have done differently to protect her privacy?
    i. Possible response: She should have left out any information that reveals personal details, e.g., where her house is, what her plans are, when her birthday is, and places she likes to go.

Recognize Harmful Content and Scams (15 minutes):

a. Divide the class into groups (three to four students per group).
b. Give each group a Scam/Dangerous Content Scenario.
c. Groups read their scenario and decide what they think the best response would be.
d. Each group shares their scenario and their response.
e. After each presentation, lead a brief positive discussion on that groups response and if anyone would change or add anything to it.

Conclusion (5 minutes):

a. Review key points of the lesson.

Assessment:

a. Take an informal assessment based on student participation and responses to scenarios.

Scam/Dangerous Content Scenarios:

Scenario 1: Fake Bank Alert
You receive an email:
Subject: "URGENT: Suspicious Activity Detected on Your Account!"

Email Body:

Dear Customer,

We have detected unusual activity on your account. For your safety, please verify your account details immediately by clicking the link below:

Click here to verify your account

If you do not verify within 24 hours, your account will be locked.

Best regards,
Your Bank's Security Team

Red Flags:

- The email creates urgency ("immediate action required").
- The sender's email address does not match the official bank's domain.
- Generic greeting ("Dear Customer" instead of your name).
- Suspicious link asking for personal information.

Scenario 2: Prize or Lottery Scam
You receive an email:
Subject: "Congratulations! You've Won a $1,000 Gift Card!"

Email Body:
Congratulations! You've been randomly selected to receive a $1,000 gift card. To claim your prize, please click the link below and provide your shipping information:

Claim My Prize
Hurry, your offer expires in 48 hours!

Red Flags:

- You did not enter any contest or lottery.
- The offer seems too good to be true.
- Urgency to act quickly.
- The sender's email is unfamiliar or suspicious.

Scenario 3: Fake Social Media Login Request
You receive an email:
Subject: "Action Required: Unusual Login Attempt Detected"

Email Body:
Dear User,
We noticed an unusual login attempt on your social media account. If this was not you, please verify your account immediately:

Verify Account
If no action is taken, your account will be temporarily suspended.

Red Flags:

- Link directing you to a fake login page to steal your credentials.
- Generic greeting like "Dear User" instead of your name.
- No specific details about the "unusual" login (like time or location).

Scenario 4: Fake Charity Donation
You receive an email:
Subject: "Help Victims of Recent Disaster – Donate Now!"

Email Body:
Dear Friend,
We are raising funds to help the victims of the recent natural disaster. Your contribution can make a difference. Click the link below to donate now:

Donate to Help
Thank you for your generosity.

Red Flags:

- The email preys on emotions to prompt quick action.
- The charity or organization is unfamiliar or does not exist.
- Link directs to a fake website designed to collect credit card information.

Scenario 5: Apple/Google Account Phishing
You receive an email:
Subject: "Your Apple ID is locked"

Email Body:
Dear Customer,
Your Apple ID has been locked for security reasons. Please verify your identity and unlock your account by clicking on the link below:

Unlock Apple ID
Failure to verify within 24 hours will result in permanent account lock.

Red Flags:

- Link to a fake login page mimicking Apple's site.
- Threatens account suspension if no action is taken.
- The sender's email address looks fake (e.g., "apple-support@randomdomain.com").

Scenario 6: Fake Streaming Service Account Alert
You receive an email:
Subject: "Your Subscription Will Be Cancelled – Update Payment Information!"

Email Body:
Dear Customer,
We were unable to process your payment for your streaming service. Your subscription will be canceled within 24 hours unless you update your payment details. Please click the link below to update your information:

Update Payment Info
Thank you for being a valued customer.
Best,
Streaming Service Support Team

Red Flags:

- Urgency: The email creates pressure with a 24-hour time limit, pushing the user to act without thinking.
- Generic greeting: "Dear Customer" instead of addressing the recipient by name.
- Suspicious link: Hovering over the link shows it does not lead to the official website.
- Unfamiliar sender: The email comes from an address like "support@streaming-service123.com," which does not match the official site.

Scenario 7: Fake School Email Asking for Personal Info
You receive an email:
Subject: "URGENT: School Needs Your Parent's Information"

Email Body:
Dear Student,
We are updating our school records and need to confirm your parent or guardian's contact details, including full name, phone number, and Social Security number. Please fill out the form linked below to ensure you stay enrolled:

Update Information
This is a required step to avoid issues with your registration.
Best regards,
School Administration Team

Red Flags:

- Personal Information Request: Schools will never ask for sensitive information like Social Security numbers through email.
- Threat of Consequences: The message says it is "required" to scare students into compliance.
- Unusual Request: Schools will ask parents to verify info, not students.
- Suspicious Link: The link leads to an unfamiliar form, not the school's official website.

Scenario 8: Fake Online Shopping Coupon
You receive an email:
Subject: "Exclusive Offer: Get 75% Off Your Favorite Clothing Brands!"

Email Body:
Congratulations! You've been selected for an exclusive offer! Get 75% off all items at your favorite clothing stores when you click below:

Claim Your Offer
This offer is only valid for the next 12 hours. Don't miss out!

Red Flags:

- Sounds Too Good to be True: Huge discounts like "75% off" are often fake, especially from unfamiliar sources.
- Time Pressure: The offer is only valid for "12 hours," making users rush to click without verifying.
- Suspicious Link: The link does not lead to the official store but to a third-party website.
- Unfamiliar Sender: The email comes from an address unrelated to any well-known store.

Grade 8

TOC Title: G8 Digital Citizenship
Lesson Title: Digital Citizenship
Grade Level: 8
Duration: 40 minutes

Objective:

- The students will understand important aspects of digital citizenship, including online safety, respectful behavior, and digital footprints.

Suggested Materials:

- Whiteboard or chalkboard.
- Paper and pens.
- A set of cards or printouts with different Digital Drama scenarios (provided below).

Procedure

Introduction (10 minutes)

a. Whole group discussion: Ask students who is on social media, and who plays games online.
b. Point out that being online makes them digital citizens. Ask students to share what they think it means to be a good digital citizen.
c. Briefly explain the concept of digital citizenship:
    i. Being a digital citizen means using technology responsibly. It is about knowing how to stay safe, being kind online, and using the Internet in helpful and respectful ways.
d. Key points to cover:
    i. Online Safety: protecting personal information and recognizing scams.
    ii. Respectful Behavior: no cyberbullying, no inappropriate comments or content.
    iii. Digital Footprint: what we post online stays there and affects our reputation.
    iv. Responsibility: using the Internet for good — learning, and making positive, appropriate connections.

Activity: Digital Drama Challenge (25 minutes)

a. Divide the class into groups of 3–4.
b. Give each group a “Digital Drama” scenario card.
c. **Group Discussion (10 minutes)**: Each group:
    i. Reads their scenario aloud.
    ii. Identifies what the problem is in terms of digital citizenship.

    iii. Brainstorms a solution or response to the situation and writes their ideas down on paper as they work.

d. **Sharing (15 minutes)**: After the group discussion, each group presents their scenario and solution to the class. Groups will explain:

    iv. Why they chose their response.
    v. How it ties back to being a good digital citizen.

Conclusion (5 minutes):

- Reflection: Ask students to think about one thing they learned today about how to be a better digital citizen. Ask a few volunteers to share their thoughts.

Assessment:

- Take an informal assessment based on each student's participation and responses during discussions and activities.

TOC Title: G8 Cyber safety
Lesson Title: Cyber safety
Grade Level: 8
Duration: 40 minutes

Objective:

- The students will understand key concepts of cyber safety.
- The students will be able to make safe decisions in a digital world.

Suggested Materials:

- Whiteboard/chalkboard.
- Paper and pens/pencils.
- Short cyber safety video. Suggestion Digital Defenders: Navigating Online Safety in Middle School, https://www.youtube.com/watch?v=zOirDXx3OJg&t=127s (2 minutes 7 seconds)
- Printed scenarios for cyber safety relay activity (provided below), or a similar age-appropriate video

Procedure

Introduction (5 minutes):

a. Whole group discussion: Ask students if they have used the Internet this week, and if so, what they did online.
b. Ask what they think some of the risks are online.
c. Explain that cyber safety means protecting yourself and your information online.

Cyber Safety Discussion (10 minutes):

a. Optional: Show a short video (around 2–3 minutes) about cyber safety.
b. Lead a brief discussion on the key points made in the video.
c. If not showing a video: Prepare a short scenario for students to read aloud and discuss. For example, Alex gets a message from someone who says they go to another school nearby. They ask for Alex's home address to send a cool gift. What should Alex do? Refer to Chapter content as needed.

Group Activity: Cyber Safety Relay (20 minutes) (Scenarios Provided Below):

a. Divide the class into 4–5 teams (depending on class size).
b. Explain the relay:
  - Each team will be given a set of cyber safety challenges on slips of paper.
  - Each slip will have a different scenario. For example:

c. Teams take turns sending one team member to pick up a slip, read it out loud, and explain how they would handle the situation.
d. The teacher or a student moderator judges whether the response is a safe choice. If it is, the team scores a point.
e. Continue until all scenarios have been addressed or the time runs out.

Conclusion (5 minutes):

a. Reinforce the day's lessons and make cyber safety memorable.
  - Recap the key points from the introduction and activity.
  - Ask students to think of one thing they will do differently online after today's lesson.

b. Key Takeaways:
  - Keep personal information private.
  - If something feels off, talk to a trusted adult.
  - Always think before you click!

Assessment:

a. Take an informal assessment based on student participation in discussions and activities.

Scenarios for Cyber Safety Relay:

Scenario 1: You receive a friend request from someone you do not know on social media. They say they know a friend of yours and want to connect.

- **Question**: What should you do?

Scenario 2: You are playing an online game and someone in the chat starts asking personal questions, like where you live and what school you go to.

- **Question**: How should you handle this situation?

Scenario 3: You get an email from a website saying your account has been hacked and you need to click a link to reset your password.

- **Question**: What is the safest way to respond?

Scenario 4: A friend sends you a link to a new app that promises to give you free in-game items. The website looks a little weird, but your friend says it worked for them.

- **Question**: Should you download the app? Why or why not?

Scenario 5: You see someone in your class being cyberbullied in a group chat. People are making mean comments and spreading rumors.

- **Question**: What should you do to help?

Scenario 6: While browsing online, a pop-up ad says you have won a free phone, but you need to provide your credit card information to claim the prize.

- **Question**: What would be the safest choice?

Scenario 7: You are at a friend's house, and they suggest sharing each other's passwords for fun, so you can log in to each other's social media accounts.

- **Question**: How should you respond?

Scenario 8: Someone sends you a direct message asking for a picture of you that you are not comfortable sharing. They say it is "just for fun" and will not show anyone.

- **Question**: What should you do?

Scenario 9: You come across a website that has disturbing or inappropriate content. It makes you uncomfortable, but you are not sure if you should tell anyone.

- **Question**: What is the best course of action?

Scenario 10: You use the same simple password (your pet's name) for all your online accounts because it is easy to remember.

- **Question**: Is this safe? What can you do to improve your online security?

Notes

1 U.S. Department of Education, Office of Safe and Supportive Schools, January 19, 2024, “Cyber Safety For K—12 Schools and School Districts,” Readiness and Emergency Management for Schools (REMS) TA Center, https://rems.ed.gov/cybersafety#:~:text=Threats%20in%20an%20online%20environment,decreased%20academic%20achievement%20by%20students, retrieved September 4, 2024.

2 JPMorgan Chase Bank, 2024, “How to Check If a Website Is Legit,” JPMorgan Chase Bank, N.A, www.chase.com/personal/credit-cards/education/basics/how-to-check-if-a-website-is-legit, retrieved September 8, 2024.

3 NCDIT, 2024, “Online Safety Tips for Teens,” North Carolina Department of Information Technology (NCDIT), https://it.nc.gov/resources/online-safety-privacy/tips-guidance/online-safety-tips-teens, retrieved September 8, 2024.

4 U.S. Department of Health and Human Services, 2024, “What Is Cyberbullying,” StopBullying.gov, www.stopbullying.gov/cyberbullying/what-is-it, retrieved September 4, 2024.

5 Office of the Surgeon General, 2023, “Social Media and Youth Mental Health: The U.S. Surgeon General’s Advisory [Internet],” US Department of Health and Human Services, https://pubmed.ncbi.nlm.nih.gov/37721985/, retrieved September 9, 2024.

6 Aichner, T., Grünfelder, M., Maurer, O., & Jegeni, D., 2021, “Twenty-Five Years of Social Media: A Review of Social Media Applications and Definitions from 1994 to 2019,” *Cyberpsychology, Behavior and Social Networking*, 24(4), 215–222. https://doi.org/10.1089/cyber.2020.0134, retrieved September 10, 2024.

7 Riehm, K.E., Feder, K.A., Tormohlen, K.N., Crum, R.M., et al., 2019, “Associations between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth” *JAMA Psychiatry*, 76(12), 1266–1273. https://doi.org/10.1001/jamapsychiatry.2019.2325, retrieved September 9, 2024.

8 The U.S. Surgeon General, 2023, “Social Media and Youth Mental Health,” The U.S. Surgeon General’s Advisory, www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf, retrieved September 4, 2024.

9 Uhls, Y. T., Ellison, N. B., & Subrahmanyam, K., 2017, “Benefits and Costs of Social Media in Adolescence,” *Pediatrics*, 140 (Suppl 2), S67–S70. https://doi.org/ 10.1542/peds.2016-1758E, retrieved September 4, 2024.

10 The U.S. Surgeon General, 2023, “Social Media and Youth Mental Health,” The U.S. Surgeon General’s Advisory, www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf, retrieved September 4, 2024.

11 Office of Communications, March 29, 2023, “Children and Parents: Media Use and Attitudes,” UK Office of Communications (Ofcom), www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf, retrieved September 11, 2024.

12 Weir, K., September 1, 2023, “Social Media Brings Benefits and Risks to Teens. Psychology Can Help Identify a Path Forward,” *American Psychological Association, Monitor on Psychology*, 54(6), Print version: page 46, www.apa.org/monitor/2023/09/protecting-teens-on-social-media#:~:text=The%20potential%20risks%20of%20social,1649%2C%202022), as found in Orben, A., Przybylski, A.K., Blakemore, S.J., et al., March 28, 2022, “Windows of Developmental Sensitivity to Social Media,” *Nature Communication*, 13(1649). https://doi.org/10.1038/s41467-022-29296-3, retrieved September 9, 2024.

13 SWNS., August 16, 2024, “Why 3 in 4 Gen Z Blame Social Media for Their Mental Health Decline,” https://nypost.com/2024/08/16/lifestyle/why-3-in-4-gen-z-blame-social-media-for-their-mental-health-decline/ retrieved September 9, 2024.

14 Wachs, S., Costello, M., Wright, M., Flora, K., et al., 2012, “DNT LET ’EM H8 U!”, *Computers & Education*, 160, 104026, ISSN 0360-1315, https://doi.org/10.1016/j.compedu.2020.104026, www.sciencedirect.com/science/article/pii/S0360131520302244, retrieved September 9, 2024.

15 Weir, K., September 1, 2023, “Social Media Brings Benefits and Risks to Teens. Psychology Can Help Identify a Path Forward,” *Monitor on Psychology, American Psychological Association*, 54(6), Print version: page 46, www.apa.org/monitor/2023/09/protecting-teens-on-social-media, retrieved September 9, 2024.

16 The American Psychological Association, May 2023, “Health Advisory on Social Media Use in Adolescence,” the American Psychological Association. www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use, retrieved September 10, 2024.

17 U.S. Department of Homeland Security, 2024, “Top 10 Tips2Protect for Teens,” U.S. Department of Homeland Security (DHS), www.dhs.gov/sites/default/files/2024-09/24_0920_k2p_top-10-tips2protect-teens.pdf, retrieved September 4, 2024.

18 (n.a.), May 2024, “Screen Time and Children,” American Academy of Child and Adolescent Psychiatry, www.aacap.org/AACAP/Families_and_Youth/Facts_for_Families/FFF-Guide/Children-And-Watching-TV-054.aspx, retrieved September 13, 2024.

19 Evans, M., 2024, “How to Talk with Kids about Inappropriate Content Online,” Verizon News Center, www.verizon.com/about/parenting/how-talk-kids-about-inappropriate-content-online, retrieved September 13, 2024.

20 Our Rescue, 2024, “Start Talking: A Guide to Keeping Children Safe Online,” Our Rescue, https://ourrescue.org/files/OURRescue_Start-Talking.pdf, retrieved September 13, 2024.

21 Governor’s Office of Information Technology, November 19, 2020, “Two-Factor Authentication (2FA) Is the Extra Layer of Security Our Customers Need in COVID Times,” State of Colorado, https://oit.colorado.gov/blog-post/two-factor-authentication-2fa-is-the-extra-layer-of-security-our-customers-need-in-covid, retrieved September 5, 2024.

22 Marcella, A., 2024, “Privacy via Two-Factor Authentication (2FA)”, Figure 2.1, graphic drawn by author.

23 Marcella, A., 2024, “Example Phishing Email,” Figure 2.2, email received by the author on May 12, 2021.

24 Marcella, A., 2024, “Example Blackmail Email,” Figure 2.3 email received by the author on June 5, 2022.

25 OIG, 2024, “Scam Alert: Pig Butchering,” Office of the Inspector General, https://www.fdicoig.gov/sites/default/files/document/2024-05/Scam%20Alert%20Flyer_Consumer.pdf, retrieved September 22, 2024.

26 Marcella, A., 2024, “Steps in Conducting a “Pig Butchering” Scam,” Figure 2.4, developed and drawn by authors.

27 CISA, 2024, “Recognize and Report Phishing,” The Cybersecurity and Infrastructure Security Agency (CISA), U.S. Department of Homeland Security, www.cisa.gov/secure-our-world/recognize-and-report-phishing, retrieved September 15, 2024.

28 NCDIT, 2024, “Avoiding Phishing Attacks,” North Carolina Department of Information Technology, https://it.nc.gov/resources/online-safety-privacy/tips-guidance/avoiding-phishing-attacks, retrieved September 15, 2024.

29 Chapekis, A., Bestvater, S., Remy, E., & Rivero, G., May 17, 2024, “When Online Content Disappears,” Pew Research Center, www.pewresearch.org/data-labs/2024/05/17/when-online-content-disappears/#:~:text=various%20online%20spaces.-,Webpages%20from%20the%20last%20decade,accessible%20just%20two%20years%20later, retrieved September 16, 2024.

30 Our Rescue, 2024, “Start Talking: A Guide to Keeping Children Safe Online,” Our Rescue, https://ourrescue.org/files/OURRescue_Start-Talking.pdf, retrieved September 13, 2024.

31 Our Rescue, 2024, “Start Talking: A Guide to Keeping Children Safe Online,” Our Rescue, https://ourrescue.org/files/OURRescue_Start-Talking.pdf, retrieved September 13, 2024.

32 Admin, June 17, 2024, “How Long Does Information Stay on the Internet?” TechGuide, www.techguide.com.au/news/internet-news/how-long-does-information-stay-on-the-internet/#:~:text=The%20short%20answer%20for%20this,data%20collection%20is%20big%20business, retrieved September 16, 2024.

33 Bapaye, J. A., & Bapaye, H. A., January 30, 2021, “Demographic Factors Influencing the Impact of Coronavirus-Related Misinformation on WhatsApp: Cross-Sectional Questionnaire Study,” *National Library of Medicine, JMIR Public Health Surveillance*, 7(1), e19858. https://doi.org/10.2196/19858. PMID: 33444152; PMCID: PMC7850780, www.ncbi.nlm.nih.gov/pmc/articles/PMC7850780/, retrieved September 18, 2024.

34 Hernandez, C., 2017, “Fake News and Information Literacy: Creating Resources to Develop Source Evaluation Skills at the University of Oregon Libraries,” *OLA Quarterly*, 23(1), 13–15. https://doi.org/10.7710/1093-7374.1885, retrieved, September 19, 2024.

35 Huang, Y., July 2021, “The New Reality: Mitigating the Risks of Misinformation,” iResearch Services, www.iresearchservices.com/wp-content/uploads/2022/10/Mitigating-the-Risks-of-Misinformation.pdf, retrieved June 9, 2024.

36 Herold, B., December 14, 2016, “Students Have Struggled with Fake News for Longer than You Think,” PBS News, www.pbs.org/newshour/education/fake-news-bogus-tweets-raise-stakes-media-literacy, retrieved September 18, 2024.

37 Caulfield, M., June 19, 2019, “SIFT (The Four Moves),” Figure 2.5, used with permission under a Creative Commons Attribution 4.0 International License [https://creativecommons.org/licenses/by/4.0/]; the authors modified the original color figure to comply with the Publisher’s grayscale requirement for figures, https://hapgood.us/2019/06/19/sift-the-four-moves, retrieved September 19, 2024.

38 Herold, B., December 14, 2016, “Students Have Struggled with Fake News for Longer than You Think,” PBS News, www.pbs.org/newshour/education/fake-news-bogus-tweets-raise-stakes-media-literacy, retrieved September 18, 2024.

39 Instagram, 2020, “Vaccines Now Injected into Meat to Get You Vaccinated!” Figure 2.6, obtained from author, www.instagram.com/reel/C-Qo0kASpBd/?igsh=MW16Nm5jdzZlbXB4Zg%3D%3D, retrieved September 19, 2024.

40 Kumar, S., & Shah, N., April 28, 2018, “False Information on Web and Social Media: A Survey,” Cornell University, https://arxiv.org/pdf/1804.08559.pdf, retrieved September 18, 2024.

41 Office of Communications, March 29, 2023, “Children and Parents: Media Use and Attitudes,” UK Office of Communications (Ofcom), www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf, retrieved September 11, 2024.

42 Akhtar, Z., January 2023, “Deepfakes Generation and Detection: A Short Survey,” *Journal of Imaging*, 9(1), 18. https://doi.org/10.3390/jimaging9010018. PMID: 36662116; PMCID: PMC9863015, www.ncbi.nlm.nih.gov/pmc/articles/PMC9863015, retrieved September 20, 2024.

43 McAfee, 2023, Artificial Imposters—Cybercriminals Turn to AI Voice Cloning for a New Breed of Scam, www.mcafee.com/blogs/privacy-identity-protection/artificial-imposters-cybercriminals-turn-to-ai-voice-cloning-for-a-new-breed-of-scam/, retrieved September 20, 2024.

44 Vosoughi, S., et al., March 9, 2018, “The Spread of True and False News Online,” *Science*, 359(3680), 1146–1151, www.science.org/doi/10.1126/science.aap9559, retrieved September 20, 2024.

45 NAMLE, 2024, “Media Literacy Defined,” The National Association for Media Literacy Education, https://namle.org/resources/media-literacy-defined/, retrieved September 18, 2024.

46 The National Institutes of Health (NIH), 2024, “The Adolescent Brain Cognitive Development (ABCD) StudySM,” U.S. Department of Health & Human Services (HHS), Figure 2.7, https://abcdstudy.org/wp-content/uploads/2023/02/Screen-Time-ENGLISH.pdf, retrieved September 4, 2024.

47 Qi, J., Yan, Y., Yin, H., April 19, 2023, “Screen Time among School-Aged Children of Aged 6–14: A Systematic Review,” *Global Health Research and Policy*, https://doi.org/10.1186/s41256-023-00297-z, retrieved September 5, 2024.

48 The National Institutes of Health (NIH), 2024, “The Adolescent Brain Cognitive Development (ABCD) StudySM,” U.S. Department of Health & Human Services (HHS), Figure 2.8, https://abcdstudy.org/wp-content/uploads/2023/02/Screen-Time-ENGLISH.pdf, retrieved September 4, 2024.

49 Marcella, A., 2024, Figure 2.9 recreated and produced by authors based on data from Duarte, F., November 10, 2023, "Average Screen Time for Teens (2024)", Exploding Topics, https://explodingtopics.com/blog/screen-time-for-teens, retrieved June 11, 2024.

50 Ofcom, March 29, 2023, "Children and Parents Media Use and Attitudes Report," The Office of Communications (UK), Figure 2.10 produced by authors based upon data presented in the Ofcom report, page 35, www.ofcom.org.uk/siteassets/resources/documents/research-and-data/media-literacy-research/children/childrens-media-use-and-attitudes-2023/childrens-media-use-and-attitudes-report-2023.pdf?v=329412, retrieved September 21, 2024.

51 U.S. Department of Education, Office of Safe and Supportive Schools, January 19, 2024, "Cyber Safety For K—12 Schools and School Districts," Readiness and Emergency Management for Schools (REMS) TA Center, https://rems.ed.gov/cybersafety#:~:text=Threats%20in%20an%20online%20environment,decreased%20academic%20achievement%20by%20students, retrieved September 4, 2024.

52 Patchin, J. W., & Hinduja, S., 2020, "Sextortion among Adolescents: Results from a National Survey of U.S. Youth," *Sexual Abuse*, 32(1), 30–54. https://doi.org/10.1177/1079063218800469, https://journals.sagepub.com/doi/abs/10.1177/1079063218800469?journalCode=saxb, retrieved September 21, 2024.

53 Strasburger, V. C., Zimmerman, H., Temple, J. R., & Madigan, S., May 2019, "Teenagers, Sexting, and the Law," *Pediatrics*, 143(5), e20183183. https://doi.org/10.1542/peds.2018-3183, www.jahonline.org/article/S1054-139X(19)30509-9/fulltext, retrieved September 21, 2024.

54 Patchin, J., & Hinduja, S., September 2018, "Sextortion among Adolescents: Results from a National Survey of U.S. Youth," *Sexual Abuse a Journal of Research and Treatment*, https://journals.sagepub.com/doi/full/10.1177/1079063218800469, retrieved September 21, 2024.

55 Criminal Division DoJ, August 11, 2023, "Citizen's Guide to U.S. Federal Law on Child Pornography," U.S. Department of Justice (DoJ) Criminal Division, www.justice.gov/criminal/criminal-ceos/citizens-guide-us-federal-law-child-pornography, retrieved September 21, 2024.

56 Canadian Ministry of Justice, June 20, 2024, Criminal Code (R.S.C., 1985, c. C-46), Publication, etc., of an intimate image without consent, https://laws-lois.justice.gc.ca/eng/acts/C-46/section-162.1.html, retrieved September 24, 2024.

57 United Nations Office on Drugs and Crime, July 22, 1992, "French Penal Code," UNODC, https://sherloc.unodc.org/cld/uploads/res/document/french_penal_code_html/french_penal_code.pdf, retrieved September 24, 2024.

58 Federal Ministry of Justice, November 22, 2021, "German Criminal Code (Strafgesetzbuch – StGB)," Federal Office of Justice, www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.pdf, retrieved September 24, 2024.

59 India Central Government, October 17, 2000, House of Parliament, "The Information Technology Act, 2000, Chapter 11, Section 66E," United Nations Office on Drugs and Crime, https://sherloc.unodc.org/cld/uploads/res/the-information-technology-act--2000_html/The_Information_Technology_Act_2000_including_amendments.pdf, retrieved September 24, 2024.

60 Department of Internal Affairs, August 26, 1993, "Films, Videos, and Publications Classification Act 1993," New Zeeland Legislation, www.legislation.govt.nz/act/public/1993/0094/latest/whole.html?search=sw_096be8ed81d31be2_inappropriate+content_25_se&p=1#DLM313407, retrieved September 24, 2024.

61 Parliament of the Republic of South Africa, 2009, "Films and Publications Amendment Act, 2009, Chapter 6, Sections 24A, paragraph 4," United Nations Office on Drugs and Crime, https://sherloc.unodc.org/cld/uploads/res/document/zaf/2002/electronic_communications_and_transactions_act_25_of_2002_html/film-and-publications-act-2008-1.pdf, retrieved September 24, 2024.

62 Republic Of Singapore, November 15, 2014, “Protection from Harassment Act 2014, PART II, Articles 3–8,” https://sherloc.unodc.org/cld/document/sgp/2014/protection_from_harassment_act_2014.html?, retrieved September 24, 2024.

63 United Kingdom of Great Britain and Northern Ireland, “Sexual Offences Act 2003,” United Nations Office on Drugs and Crime, https://sherloc.unodc.org/cld/uploads/res/document/gbr/2000/sexual-offences-act-2003_html/Sexual_Offences_Act_2003.pdf, retrieved September 24, 2024.

64 U.S. Department of Education, Office of Safe and Supportive Schools, January 19, 2024, “Cyber Safety for K—12 Schools and School Districts,” Readiness and Emergency Management for Schools (REMS) TA Center, https://rems.ed.gov/cybersafety#:~:text=Threats%20in%20an%20online%20environment,decreased%20academic%20achievement%20by%20students, retrieved September 4, 2024.

65 National Center for Missing & Exploited Children, 2024, “Online Enticement,” National Center for Missing & Exploited Children, www.missingkids.org/theissues/onlineenticement, retrieved September 4, 2024.

66 United States Government Accountability Office, 2014, “Child Welfare Federal Agencies Can Better Support State Efforts to Prevent and Respond to Sexual Abuse by School Personnel, Report to the Ranking Member, Committee on Education and the Workforce, House of Representatives,” www.gao.gov/assets/gao-14-42.pdf, retrieved September 4, 2024.

67 Polanco-Levicán, K., & Salvo-Garrido, S., July 20, 2022, “Understanding Social Media Literacy: A Systematic Review of the Concept and Its Competences,” *International Journal of Environmental Research and Public Health*, 19(14), 8807. https://doi.org/10.3390/ijerph19148807. PMID: 35886657; PMCID: PMC9325204, www.ncbi.nlm.nih.gov/pmc/articles/PMC9325204/#:~:text=It%20is%20understood%20as%20the,in%20a%20variety%20of%20contexts, retrieved September 22, 2024.

68 Bauld, A., 2024, “15 Important Trends in Education,” XQ Institute, https://xqsuperschool.org/teaching-learning/15-important-trends-in-education, retrieved August 31, 2024.

69 Office of Communications, March 29, 2023, “Children and Parents: Media Use and Attitudes,” UK Office of Communications (Ofcom), www.ofcom.org.uk/__data/assets/pdf_file/0027/255852/childrens-media-use-and-attitudes-report-2023.pdf, retrieved September 11, 2024.

70 Cukurova, M., & Luckin, R., 2018, “Measuring the Impact of Emerging Technologies in Education: A Pragmatic Approach,” https://discovery.ucl.ac.uk/id/eprint/10068777/1/Methods%20to%20measure%20emerging%20technology%20impact_Final.pdf, retrieved August 31, 2024.

3

STRANGERS

Safe/Unsafe People and the Tricky Person

Why Someone Known Isn't Always Safe

As children move into their teens and become more independent, personal safety becomes a more important concern. Interpersonal interactions become more frequent and are less supervised or monitored.

Who Is a Tricky Person?[1]

According to Internet Matters, nearly one-third of preteens say they are not sure if all they see online is true, and one in four indicates that a stranger has contacted them.[2] How do we connect these perceptions with the reality — that there is often a deception in trust when online? (Figure 3.1)

Figure 3.1 Who is behind the screen?[3]

DOI: 10.1201/9781003466376-3

At one time, it was considered that danger came in the form of a stranger, but danger may also be encountered as someone known to the child, and often known to the family, using both terms, tricky and unsafe people, speaks to actions and less about the relationship involved. Teens may be tricked by both the stranger and someone they know.

According to the Centers for Disease Control and Prevention (CDC), someone known and trusted by the child or child's family members perpetrates 90% of child sexual abuse.[4] This leaves only 8% perpetrated by a person unknown to the child.

Going back to the Chapter 1 ethics discussion, acting ethically in all situations and activities is a good start to keeping you and others cyber-safe while online. A solid start to protect oneself is by not engaging with anyone online you don't know.

Who Is and Is Not a Tricky or Unsafe Person?

As children grow and online exposure and use increases, talking about tricky people becomes a critical and regular conversation to reinforce its importance. Online activity and the opportunity to connect and communicate with people we do not know are redefining our ideas of connection and relationships.

Social interactions via online social networking sites and online chat rooms have now become a means for filling social gaps or social isolation.

Additional Interests to Address

Planet Puberty, a digital resource suite by Family Planning NSW, aims to provide parents and carers of children with intellectual disability and/or autism spectrum disorder with the latest information, strategies, and resources for supporting their child through puberty. Planet Puberty's focus is on children with intellectual disability and autism spectrum disorder; the list of rules for tricky people may be used in that environment and is also applicable to all children.

The following are some rules for children with intellectual disability and autism spectrum disorder about "tricky people" (summarized from the Safely Ever After Program).

1. People must ask your permission before touching you in any way. This includes hugs and kisses. The child does not need to apologize or have a reason for not wanting to hug or kiss someone.
2. Everybody has private body parts that must be covered when you are in public.
3. Your child should never go anywhere with someone they don't know or take anything from someone they don't know.
4. Children should always check with their parents/carers before
    - changing plans without prior notice,
    - getting into a car (even if the driver is someone they know), and
    - accepting gifts (gifts should never be a secret).

5. Your child does not have to be polite if they feel scared or uncomfortable.
6. Your child is allowed to say or sign NO to adults and other children.
7. No, Go, Tell: Teach children to say or sign no, and then go and tell their safe people.
8. Children should never be asked to keep a secret, unlike a surprise. Adults should never ask children to keep a secret.[5]

Activity

Have students identify what makes them feel safe when they are online. Encourage students to share their ideas of safe people using the concept of feelings and actions rather than names and titles.

If negative or unsafe ideas are communicated, talk about the opposite — what can make that safe? An example could be someone sending them pictures that make them uncomfortable. Feeling safe can include talking about how they have the power and the right to say "Stop!" or "I am not comfortable with those pictures, please stop sending them." Talk about blocking people. "I feel safe knowing I can block those who do not respect me and make me feel uncomfortable."

Create a classroom list of safe people and, if possible, display it as a reminder. Continue supporting good and positive examples.

Teachers can be a safe and trusted adult for children. Let them know you are there for them. Be sure you are added to the list of safe people.

Morrisa Berkley, Certified Holistic Life Coach and, Founder at Love One Inc., states,

> I can't tell you how many conversations I have had with adults who experienced abuse as a child or youth and either did not feel safe enough to tell someone, or when they did, they were not believed or blamed. This is so powerful and sorely needed.

Darkness to Light, an organization with the mission to end child sexual abuse, provides methods for you to be a safe adult — so that a child can trust you to be there for them when they need help.

- Set and maintain clear, protective boundaries. This is a crucial step because boundaries help us to respect each other and feel respected. A child who knows that you will respect (and even protect!) their boundaries will have an easier time trusting you to take care of them.
- Develop protective bonds. Really listen when the child talks to you. Show them that you're interested in their opinion; involve them in conversations and show them that their input is valuable.
- In appropriate settings, talk openly and honestly about child sexual abuse. When we talk to children in age-appropriate ways about our bodies, sex, and boundaries, children understand what healthy relationships look like. It also teaches them that they have the right to say "no."[6]

Because of the conflicted parent- or guardian–child relationship or due to a specific threat against telling them, the child may feel like there is nowhere to turn. As a trusted adult, you may be able to assist children in developing an awareness of unsafe or tricky people, or in directly helping remove the child from the situation.

The nonprofit, Operation250, whose organizational goals are to keep youth safe from threats and malevolence online, talks about predators. Predators, also known as online groomers and online recruiters, are given almost unlimited Internet access to their target audience. Anyone, particularly a technology-savvy adult, can quickly create a full user profile complete with a name, pictures, location, and school, and be quite convincing.

The average teenager is now spending upward of 9 hours a day on the Internet or on their mobile device, which is situationally optimal for online recruiters. When a child is being radicalized or groomed, they will be showered with attention or connected with their recruiter very often. This is done quite purposefully on the part of the recruiter. Remaining in constant contact with their recruit allows the recruiter to

- fill an emotional void within the child (doing this will make the child easier to manipulate, and likely far more willing to continue the relationship with the recruiter),
- isolate them from their physical lives by keeping them attached to technology, and
- hasten the indoctrination process.[7]

Important — if you suspect or know that inappropriate exchanges are taking place:

- Schools, child-serving organizations, caregivers, etc. should notify the administration and contact the child's guardian immediately.
- If the exchange is taking place on school grounds, check your organization's policy as you may have an obligation to contact your local law enforcement agency and/or the Federal Bureau of Investigation (FBI).
- Parents and guardians, contact your local law enforcement agency and/or the FBI.
- You may contact the FBI using the cited form.[8]

Gaming and Avatars — What's Safe, What's Not

Experience with online games is now rather routine for most early teens and many have an avatar, i.e., a representation of themselves. Microsoft posts this reminder: Once something is shared on the Internet, it's almost impossible to fully erase it.[9]

What You Post

We know it can be difficult, if not impossible, to get out of something once you have entered into it. This is particularly true once anything is posted and shared online via social media apps, discussion boards, and other sharing services. Chapter 1 discussed the "cost" of making decisions, and social media is the strongest example of where the cost could last forever — even if the teen user is only thinking about NOW.

An example of the perpetuity of data and a good opportunity to discuss how permanent data is when posted on various websites, with your students, is The Wayback Machine.[10] This is an initiative of the Internet Archive,[11] a 501(c)(3) nonprofit, which is building a digital library of Internet sites and other cultural artifacts in digital form.

The Internet Archive began in 1996 by archiving the Internet itself, a medium that was just beginning to grow in use at that time, and anyone with a free account can upload media to the Internet Archive.

Although it has been around for a while, doxing (or sometimes seen as doxxing) is now seen more often. It is a form of cyberbullying that uses sensitive or secret information, statements, or records for harassment, exposure, financial harm, or other exploitation of targeted individuals. It involves taking specific information about someone and then spreading it around the Internet as a means of getting it out to the public.[12] With content on the Internet remaining "forever," these schemes do not have an expiration date.

The Department of Homeland Security (DHS) Digital Safety Series shares the following message:

> We're really trying to reinforce that any app, any social media, any game that has a communication feature where someone from the outside world can communicate with a child there's a vulnerability in that app.
>
> So, you cannot rely on the app or the technology to protect your kid, that you are going to have to be the one that does the research. You've got to get involved. You've got to make sure that things are appropriate and that their friends lists are checked. The people they are playing games with are checked.
>
> We don't want to be the boogeyman. We're not trying to say that it's doom and gloom everywhere, but the fact of the matter is that there's really no technology that is 1,000% safe for kids.[13]

DHS continues to discuss the metadata and the geolocation information while taking a picture.

As discussed in Chapter 2, this is information stored within the image. Disable location settings and confirm that no location or date/time stamps are included. DHS cautions that such information should be removed, so that information cannot be used to exploit the child.

Gaming Vodafone Limited, the British telecommunications company and the world's eighth-largest telecommunications company,[14] shines a light on what parents — and the gaming industry — can and should be doing to protect children, amid reports that VR Worlds is increasingly drawing groomers and racists.

In the United Kingdom, 80% of children aged between 12 and 15 are estimated to play online games like Fortnite or Minecraft.

Europol, the law enforcement agency of the European Union, warns that greater unsupervised Internet access during the pandemic left children "more exposed to offenders through online gaming." Some had become "lonely and isolated, which offenders try to benefit from, connecting with them to produce explicit material or to arrange a meeting in real life."[15]

An avatar is very common on social media sites, especially in gaming. As a representation of a person, it may be an expression of their interest and likes. It may even be how they see themselves, especially in online activities. It is not just a distortion of an actual photo of the individual but may also be a character or object. Not all games are bad, and neither is having an avatar (Figure 3.2).

Figure 3.2 Mystery person.[16]

Hiding behind an avatar is an ideal way for an adult to gain access to various gaming sites for children with the sole purpose of "grooming" the child for potential nefarious activity such as an in-person meeting often to commit sexual abuse.

Various apps will have a chat feature thought to be only for gamers within the app, appearing as a safe place to chat with others. However, many of these apps become a backdoor to Internet access. School devices or devices students bring from home to school or after-school activities may have websites blocked or the Internet disabled, believing the device and all apps are "safe". An app may seem child-safe, yet it allows access to other sites and to chats that are not.

Once the bad actors behind the avatar befriend the child, they invite the child to move to a different social media site. The chat feature within the app may circumvent the assigned controls. Monitoring is crucial.

Bill Sweeney, with the FBI office in New York City, cautions parents and guardians. "As soon as the "instant message" pops up on your child's browser or on their smartphone, there could be a sexual predator on the other end. It takes only a few days — sometimes just hours — to groom your child into sending compromising photos to the person on the other end of that chat. Then the threats begin. That predator starts to ask for photos of your child — something they would be ashamed of if anyone, including you, found out. Then they threaten to post them online if they don't keep sending more and more graphic photos."[17]

When predators pose as someone else online to coerce victims into taking and sending sexually explicit photos and videos — and then immediately demand payment or threaten to release the photo to the victim's family and friends — it's known as financially motivated sextortion. Financially motivated sextortion is a crime.

Parents, educators, caregivers, and young people should be aware of how to stay safe online, the risks and warning signs, and how to report if you or someone you know is a victim. According to the FBI:

- Victims are typically males between the ages of 14 and 17, but any child can become a victim.
- There have been an alarming number of suicides identified in male victims of financially motivated sextortion schemes.
- Victims often feel alone, embarrassed, and afraid to seek help. But victims need to understand they are not alone. If you're feeling threatened, ask a trusted adult for help.

Because the target victim is male, predator profiles are often made to look like teenage females. The FBI further states that predators often pretend to relate to victims, whether that's pretending to be their age, have similar interests, or live in the same area. They easily misrepresent themselves online to appear to be friendly and age-appropriate.[18]

This is a fitting time to revisit the billboard example presented earlier in the chapter and resume the discussion about why providing too much information, especially to someone you do not know or may have just met online may invite online predators.

The National Center for Missing & Exploited Children (NCMEC) released the number of financial sextortion reports received from the public and electronic service providers, broken down by month. In 2023 alone, NCMEC received 26,718 reports of financial sextortion, up from 10,731 reports in 2022[19] (see Figure 3.3).

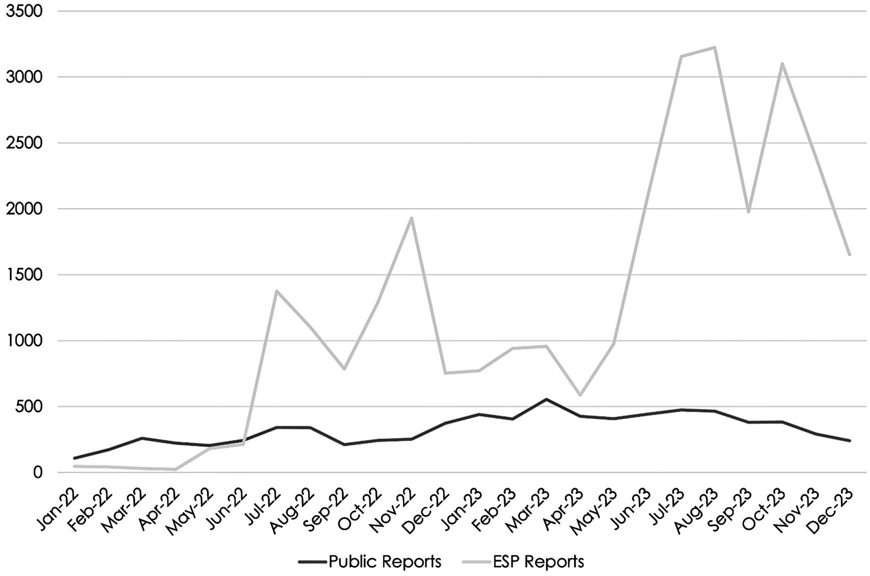


Figure 3.3 NCMEC sextortion data by month.[20]

This may leave the victim feeling alone and embarrassed for being fooled. Building trust that you are a safe person will allow the student to seek out counsel and advice.

Why Do Young People Go Online?

The Antisocial Network: Memes to Mayhem,[21] produced by Giorgio Angelini and Arthur Jones, is about a group of lonely teenagers who form an online community bonding over their isolation.

Real characters — not actors — talk about shared experiences. Although this blossomed into something unexpected, it discusses what drives young people online for social experiences. The founder of one of the largest antisocial networks, and who subsequently left (not named in the movie), indicates that "they go online to feel less alone and to simulate community when in fact you are experiencing less of life" — "you're alone together." This anonymous founder further states "go out and live your life."

Other Ways Apps Can Compromise Young Users

App developers and the companies marketing them want to sell more products, services, and other apps. Pop-up blockers are great — especially when they are used — but are not fail-safe. Many sites will ask for "demographic" information during setup or in the creation of the avatar. Site policies vary and for teachers, guardians, and parents this should be a supervised process.

According to the Washington Post article "Your Kids Apps are Spying on Them," children's privacy "deserves special attention because kids' data can be misused in some uniquely harmful ways."

Research suggests many children can't distinguish ads from content.[22] This is why kids are at the center of one of America's few privacy laws, the 1998 Children's Online Privacy Protection Act, or COPPA. Although this act has been on record since 1998, a big loophole remains.

Tech companies and app designers argue that they do not "actually" know they are taking data from kids.[23] Essentially, vetting mechanisms to confirm a child's age do not exist in most apps and there is no proof of age requirement, making it easy to falsify the user's age.

As we read in Chapter 2, apps create an ideal opportunity to provide personally identifiable information (PII). A series of questions may be asked during the setup process. Frequently, this step is not required to gain access to the app and may often be skipped. There are also many engaging and fun apps and games accessible without the Internet. Although the questions may seem innocent, the PII provided may be used by groomers to lure children to other sites.

When the questions refer to other family members, pets, and pet names, or where you live or go to school, hackers may use this information to gain access to other family members. Parental and security controls are critical to keeping young users safe from tricky and unsafe people, whether the school provides devices or students bring their own devices to school.

But are all apps bad? In January 2022, a study by the University of Trento in Italy found that gaming can boost academic achievement, exercising young people's memory, attention, and reasoning skills. Researchers studied and tested to see if instead of being an obstacle to literacy, video games could help children improve their reading abilities. Researchers tested an action video game for children, aimed to enhance reading skills. The results demonstrate improved reading abilities after just 12 hours of training. For the study, a video game was designed that combines action video games with mini-games that train different executive functions, such as working memory, inhibition, and cognitive flexibility, functions that are called upon during reading.[24]

A source for understanding the media available, at an age-appropriate level, is the nonprofit CommonSense.org. Believing that most technologies weren't built with kids in mind, Common Sense is on a mission to change that. Common Sense rates movies, TV shows, apps, podcasts, books, and more, so teachers and families can feel good about the learning and entertainment choices they make for their kids. Offering a library of independent age-based ratings and reviews helps make choices about what to play, read, and watch.[25]

Mandatory Reporters

According to REMS — Readiness and Emergency Management for Schools — which operates under contract by the US Department of Education, responsibilities exist to report suspected cases of adult sexual abuse and include online settings, sextortion, and human trafficking. Confirm your organization's policy and obligations under this requirement.

> Mandated or mandatory reporters (both terms are correct) are individuals required by state law to report abuse ("Mandatory Reporters," 2013). According to the U.S. Government Accountability Office (GAO) (2014), in most states, school personnel (including administrators, teachers, psychologists, and nurses) are considered mandatory reporters, but states vary in their designations. Mandatory reporters are generally those who have frequent contact with children. Some states have the freedom to decide who should be designated as mandatory reporters.
>
> In most states, a mandatory reporter is required to report cases of suspected adult sexual misconduct (ASM) to state or local child protection services; some state laws also require that reports be made to a designated school employee (GAO, 2014). Other states can establish their own standards for reporting child abuse or neglect. Variations in state laws are a primary consideration in the development of policies on mandatory reporting laws. Some school districts have developed formal agreements, such as a memorandum of understanding with local law enforcement agencies. Some school districts have formally required reporting for ASM crimes that happen in online settings, including sextortion and human trafficking, which are also defined in these documents as mandatory reportable incidents (Newton Public Schools, n.d.).
>
> A "permissive reporter" ("Mandatory Reporters," 2013) is an individual who is not a mandatory reporter and voluntarily reports child abuse or neglect; anyone can be a permissive reporter. In at least 18 states, however, *anyone* who suspects abuse is mandated to report it, regardless of their profession.[26]

Online Use — Teen Well-Being and Mental Health

The authors and contributors are not mental health professionals, and the following section is not mental health or medical advice. It is presented to teachers as helpful information and to create awareness of the cue's students may display when experiencing well-being trials and offers suggestions for action. These concepts and responses are designed to make you a trusted person to the students, someone who cares about them and to whom they can turn when in need, and are not a substitute for the qualified knowledge, skills, and judgment of a mental health professional.

As we discussed in other areas and shown in the film *The Antisocial Network: Memes to Mayhem*, teenagers search online communities to form relationships and to bond over their isolation. Being online becomes a social experience. They go online to feel less alone, and someone shows an interest. This is interpreted as a relationship with the potential to escalate into other activities. These activities may lead to compromised or dangerous behavior and open the door to other actions such as sexting or moving online conversations to in-person meetings with the anonymous "friend." Sexting may lead to sextortion, or they may realize that the friend is not the teen they thought they were.

As the behavior escalates, the victim may feel that they have let everyone down. The person online isn't who they said they were. The sextortion isn't stopping as promised with more pictures. Thoughts consume them. Parents and other family members will be so disappointed. They are embarrassed and feel shame — to whom can they share this? Will the authorities be involved? These online activities and traps lead to feeling overwhelmed — that there is no way out. This thinking spirals to thoughts of harming themselves or of suicide[I] as the only way to escape.

It is important to talk about well-being directly with teens. Although they may not display signs causing concern, opening this discussion builds the relationship whether for them or their friends and family who they know are at this level of distress. It lets them know that they are important, their concerns are important, and they can come to you. Many teens may not exhibit overt signs of distress. Instead, they may have subtle changes in behavior, disposition, become angry or lethargic, or there may be changes in their class work and school participation.

The CDC statistics indicate suicide rates increased by approximately 36% between 2000 and 2022. In 2022, suicide was among the top nine leading causes of death among age groups 10–64. Suicide was the second leading cause of death for ages 10–14 and 25–34.[27]

According to the CDC's National Vital Statistics System, suicide is the third leading cause of death among adolescents aged 15–19 years:

- Accidents (unintentional injuries)
- Homicide
- Suicide.[28]

The impact and scale of social media on teen mental health is at a scale that the US Surgeon General issued public advisories[29] and accelerated the concern by issuing a statement that "warning labels" should be on social media sites.[30]

More information centered on well-being and mental health is provided in Appendixes H and I. These appendices are authored by three consultants who work with adolescents and various aspects of well-being and mental health.

Appendixes H and I are not mental health or medical advice but is presented to teachers as helpful information and to create awareness of the cue's students may display when experiencing well-being trials and offers suggestions for action. The information contained is not a substitute for the knowledge, skills, and judgment of a qualified mental health professional. These concepts and responses are designed to make you a trusted person to the students, someone who cares about them and to whom they can turn when in need. If a threat is imminent, seek help immediately.

[I] References to suicide should be "suicide, suicidal ideation, thoughts of suicide, or death by suicide" as options. The mental health community strongly advocates against using "commit" with suicide.

An Additional Level of Safety — A Safe-Word

Students want to feel more independent, yet for students having trouble, trust needs to have been established before the incident for them to feel safe coming to you and talking. Creating a safe word provides a code for all situations. A safe word gives assurance that you are there to help them. It makes them feel that they have control in many situations. Many families have a safe word that is used if their child feels unsafe or uncomfortable.

A classroom safe word can be created as well. It is a word or a couple of words, and it is not shared with other classrooms. Administration may need to know your classroom save word, so they can be available to provide support if required or requested. Let students know this and gauge their comfort with extending this beyond the classroom.

Examples of using the safe word may include at a school sporting event, after-school activities, and any school-sponsored event where the child is made to feel uncomfortable by an adult or even another student.

As an exercise, role-play responses if someone they have only met online asks them for inappropriate pictures.

Note: This exercise is to stop the conversation with the perpetrator and is not the final solution. The child needs to know they must share that they have been approached with a teacher, parent or guardian. Here are some examples to which you may add yours.

What would they say?

- "I never send pictures to people I don't know."
- "I tell them not to make contact with me again."
- "I am telling my (a trusted adult – teacher, parent/guardian, sibling)."

What should they do?

- "I block them."
- "I don't know them, so I don't have to be polite."
- "I disconnect from the site immediately."
- "If there is no trusted adult and I am scared, I call the police."

Who would they tell?

- "I tell my teacher, parent/guardian, older sibling, a nearby trusted adult."
- "If I am scared and no one I trust is near, I call the police for help and let them know where I am."

What would I do if I sent them pictures and they asked for more or they threatened to release the pictures I already sent?

- "I would say NO! and not send more pictures."
- "I would take a screenshot of the message."

- "I would tell my trusted adult and ask for help. I know my trusted adult will not judge me and will help me."

Remind students about using their safe word. Mock practice ways to reach out to their trusted person. Like studying for a test, the more practice, the more likely the child will not be tricked into meeting and going anywhere with an unfamiliar person.

Important — if you suspect or know that inappropriate exchanges are taking place:

- Schools, child-serving organizations, caregivers, etc. should notify the administration and contact the child's guardian immediately.
- If the exchange is taking place on school grounds, check your organization's policy as you may have an obligation to contact your local law enforcement agency and/or the FBI.
- Parents and guardians, contact your local law enforcement agency and/or the FBI.
- You may contact the FBI using the cited form.[31]

Summary

Teens have become more independent and are familiar with more online resources. Many have mobile phones and access to apps and games online. By discussing the pitfalls that come with being online, in addition to the many benefits, they can learn to become aware and responsible users of the many online tools available. They can recognize when they are giving away too much information and the related costs. This craving for independence creates a level of confidence that may be ill-placed, and lead to spiraling mental health concerns. Knowing the warning signs that people may not be who they say they are, and that they can say "No!" is critical to navigating their online world. As their "protectors," no matter their age and desire for independence, keeping them safe online is everyone's responsibility.

Chapter 4 presents stewardship, and the emerging topic of "Exploring Cyber Safety Through Stewardship."

LESSON PLANS

Grade 7

TOC Title: G7

Lesson Title: Gaming and Avatar Safety
Grade Level: 7
Duration: 50 minutes

Objective:

- The students will understand the importance of online gaming safety.
- The student will be able to recognize the role of avatars in protecting their identity.
- The students will be able to identify safe and unsafe behaviors when interacting with others while gaming online.

Suggested Materials:

- Whiteboard/chalkboard.
- Markers or chalk.
- Blank paper or large index cards for avatar creation activity.

Procedure

Introduction (10 minutes):

a. Begin by asking students if they play online games and what games they enjoy.
b. Introduce the topic of online gaming safety, focusing on the following:
    i. The risks of sharing personal information with strangers in games.
    ii. How avatars can help protect personal identity.
    iii. The importance of knowing how to identify "safe" and "unsafe" online behavior.

Discussion on Avatars and Their Role (10 minutes):

a. Explain what avatars are in the context of online games: digital characters that players use to represent themselves.
b. Discuss how avatars help:
    i. Maintain privacy by using images instead of real photos.
    ii. Allow players to have fun expressing themselves without revealing personal details.
    iii. Establish boundaries, so players can interact without sharing personal information.

Activity: Create Your Safe Gaming Avatar (20 minutes):

Instructions:

a. Hand out blank sheets of paper or large index cards to each student.
b. Ask students to design a unique avatar that represents them but does not reveal personal information like their real face, age, or location.
c. Prompt them to think creatively about their avatar's look and personality (e.g., favorite colors, animals, or fantasy elements).
d. After designing, have students write two to three safety rules their avatar would follow in an online game, e.g., never sharing their real name or only friend people I know in real life.

Share and Reflect (5 minutes):

a. Invite a few students to share their avatars and the safety rules they have written.
b. Encourage students to discuss how using avatars and following these rules helps them stay safe online.

Conclusion (5 minutes):

a. Emphasize that avatars are a fun, creative way to play games safely and anonymously.
b. Remind students that keeping personal information private is essential, even if they feel comfortable with someone online.

Assessment:

a. An informal assessment can be taken based on avatar activity and overall engagement and participation.

TOC Title: G7 Tricky Person
Lesson Title: Tricky Person
Grade Level: 7
Duration: 40–45 minutes

Objective:

- The students will be able to differentiate between safe and unsafe online interactions.
- The students will be able to recognize characteristics and behaviors that indicate safe or unsafe online people.

Suggested Materials:

- Whiteboard/chalkboard.
- Profile cards representing different online people (suggestions below).
- A short video on tricky people online. Suggestion: Digital Citizenship for Kids: A Video about Online Strangers, https://www.youtube.com/watch?v=GQuXmAIcdCw (3 minutes 8 seconds), or another or another age-appropriate video.

Procedure

Introduction (10 minutes):

a. Whole group discussion: Ask students about the kinds of people they might encounter online, e.g., friends, family, strangers, friends of friends. Use the whiteboard/chalkboard to register ideas.
b. Review the importance of digital boundaries.
c. Explain the risks of sharing personal information with unknown people online.
d. Emphasize students' responsibility for personal and shared online safety.

Video and Discussion (5–10 minutes):

a. Show a short video related to safe/unsafe people online. Suggestion: Digital Citizenship for Kids: A Video about Online Strangers, https://www.youtube.com/watch?v=GQuXmAIcdCw, or another age-appropriate video.
b. Briefly discuss the key information in the video.

Activity (20 minutes):

a. Divide the class into groups of three to four students.
b. Explain that each group will get profile cards representing different online people.
c. Each group will discuss and decide whether each profile seems safe or unsafe, explaining their reasoning for each decision.
d. Whole group: Go through each profile and ask groups to share their thoughts. Use this activity to clarify misconceptions and reinforce safe behaviors.

Conclusion (5 minutes):

a. Reflect on why it is important to trust your instincts and ask an adult if something feels uncomfortable.
b. Encourage students to think before sharing personal details and only connect online with people they know well offline.

Assessment:

a. An informal assessment can be taken based on student participation in discussions and group activity.

"Friend or Foe?" Profile Cards:

New Friend from School

This person goes to your school but is in a different grade. They started following you on social media, have mutual friends with you, and comment positively on your posts.

Gamer Buddy

This person is someone you met while playing an online game. You have chatted with them a few times about the game, and they seem friendly. They recently asked you for your real name and where you live.

Family Friend

This person says they are a friend of your parents and followed you on social media. They send friendly messages and talk about knowing your family, but you do not remember meeting them in real life.

Fellow Hobbyist

This person joined a public group where you discuss a shared hobby, like drawing or sports. They share photos and posts about the hobby but recently messaged you privately, asking personal questions about your family and school.

"Fan" of Your Posts

This person frequently likes your photos and comments on every post, even though they are not someone you know. Recently, they sent you a private message asking if you would like to hang out in person.

New Classmate

This person claims to be a new student at your school and just sent you a friend request. They have not posted any pictures of themselves, and you do not have any mutual friends.

Friend of a Friend

This person is friends with someone you know but has never talked to you in real life. They sent you a friend request and keep trying to message you.

Online Influencer

This person is popular on social media and follows a lot of young people. They recently commented on one of your posts and messaged you to say you could "get famous" by talking with them more.

Relative in another State

This person says they are a distant cousin and sent you a message. They share some photos of family events but keep asking for more details about where you live and other family members.

Classmate's Older Sibling

This person says they are a sibling of someone in your grade. They reached out, asking if you are interested in attending a group meet-up with them and some friends.

"Friend or Foe?" Answer Key:

New Friend from School

Safe (with caution): Since they are from your school and have mutual friends, they are likely safe. However, advise students to still be cautious with sharing personal information and meet in person first if they have not already.

Gamer Buddy

Unsafe: This person is asking for personal details (like your name and location), which is a red flag, especially since they are only an online gaming contact. Remind students to keep personal information private from online-only friends.

Family Friend

Unsafe: Although they claim to know your family, if you have not met them in person and do not have a family member to confirm their identity, this could be risky. Caution students to check with their families before engaging with such people.

Fellow Hobbyist

Unsafe: While a shared hobby might feel safe, the fact that this person is asking for personal information privately indicates that they may not have good intentions. It is best to keep conversations public and avoid sharing personal details.

"Fan" of Your Posts

Unsafe: This person is overly interested in connecting and has shown inappropriate interest by asking to meet in person. Caution students against meeting online-only acquaintances without a trusted adult involved.

New Classmate

Unsafe: This person's lack of a verifiable identity (no mutual friends or real photos) is a red flag, and they could be pretending to be a peer. Students should avoid accepting connections from people who they cannot verify.

Friend of a Friend

Unsafe: Even though they are connected to someone you know, you do not have a direct relationship with them, and they have been persistent in trying to engage you. It is best to avoid close online interactions with people you do not know well personally.

Online Influencer

Unsafe: While they may seem trustworthy because they are popular, an influencer offering “fame” or wanting personal contact is usually a red flag. Students should remember that trustworthy adults and professionals don’t offer favors or promises to young people online.

Relative in another State

Potentially Unsafe: If they are truly a distant relative, they should be verifiable through family connections. Advise students to check with a family member before sharing information.

Classmate’s Older Sibling

Unsafe: Since they are a stranger and are asking to meet up, it is best to be cautious. Even if they are related to someone they know, students should avoid meeting anyone they have not met in a trusted, supervised environment.

Grade 8

TOC Title: G8 Gaming and Online Safety

Lesson Title: Gaming and Online Safety
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will understand the purpose of avatars in online gaming.
- The students will be able to identify privacy and safety risks associated with using personal information in online gaming.
- The students will know and be able to use strategies for maintaining personal safety while gaming online.

Suggested Materials:

- Whiteboard and markers.
- Printed worksheets for avatar activity (template included below).
- Optional: Colored markers/pencils for activity.

Procedure

Introduction to Online Gaming and Avatars (10 minutes):

a. Whole group discussion: Ask students if they play online games. Ask what their favorites are.
b. Ask what an avatar is, and why people use them in online games.
c. Explain avatars as a representation of oneself in the virtual world. Discuss ow they can be fun, creative, and an essential part of gaming, but are also a potential risk if they reveal too much personal information.

Understanding Privacy and Boundaries in Online Gaming (10 minutes):

a. Discuss privacy risks when sharing personal details through avatars and user profiles. Explain the importance of not using personal photos, real names, or other identifying features in avatars.
b. Optional: Show examples of safe vs. unsafe avatars (e.g., an avatar with a username like "John2011" vs. one like "RedKnight").

Activity: Create a Safe Avatar (20 minutes):

Instructions:

a. Each student will design their own safe avatar on a worksheet.
b. The avatar should avoid real-life identifiers and reflect personality or interests without revealing personal info.

c. Students should also choose a safe username that does not include their real name, age, or location.
d. If needed, offer suggestions. Tell students to think about hobbies or interests they would like to show through their avatar, or what colors or fictional traits they can add to make their avatar fun but safe.
e. Have students share their avatars with a partner and discuss the choices they made for privacy.

Conclusion (5 minutes):

a. Reinforce the importance of using avatars for privacy protection, not sharing personal information, and always reporting suspicious behavior in online games.
b. Ask students what they can do if they feel uncomfortable with someone in a game.

Assessment:

a. An informal assessment can be taken based on student participation in the activity and their ability to make safe choices in avatar creation.

Online Gaming Avatar Safety Worksheet

Instructions: Use this worksheet to design an avatar for online gaming that is fun and safe! Follow the prompts to think creatively about how you can represent yourself without giving away personal information.

Avatar Design

1. In the blank space below, draw or describe what your avatar would look like.

   Guidelines: Avoid using any personal information or images. Think about colors, shapes, and features that represent hobbies or interests without revealing personal information.

   Draw your avatar:

2. Describe your avatar.

   What features did you choose, and why? (Example: "My avatar wears a soccer jersey because I like sports, but I did not use any real team logos.")

Part 2: Choose a Safe Username

1. **Pick a Username**
   Create a username that does NOT include any of the following:
   Your real name
   Your age
   Your location
   Examples of safe usernames: FireKnight, GameNinja, AstroPenguin

2. My Username: __________________________________

Part 3: Reflection Questions

1. Why is it important not to include personal information in an avatar?

2. What would you do if someone asked you personal questions in a game?

TOC Title: G8 Tricky Person

Lesson Title: Tricky Person
Grade Level: 8
Duration: 40 minutes

Objective:

- The students will understand the concept of safe vs. unsafe people online.
- The students will be able to identify red flags in online interactions.
- The students will know and be able to use strategies for safe online engagement.

Suggested Materials:

- Whiteboard/chalkboard.
- Printed scenario slips (suggestions below).
- How to Set Healthy Personal Boundaries
  https://www.youtube.com/watch?v=pC5FtPX6Ngg (2 minutes), or another age-appropriate video.

Procedure

Introduction (10 minutes):

a. Whole group: Ask students what makes someone safe or unsafe to interact with online.
b. Write student responses on the whiteboard.
c. Briefly outline what "safe" and "unsafe" people might look like online, including examples of friendly vs. suspicious behaviors.
   i. Friendly examples may include respectful language, being honest/transparent, they are positive/supportive, having a reasonable frequency of interaction (not overbearing).
   ii. Suspicious behaviors may include being vague about their identity, asking inappropriate personal questions and pressuring you to answer them, expressing inappropriately close connection to you too quickly, ignores your boundaries.

Video and Discussion (10 minutes):

a. Show video related to the topic. Suggestion: How to Set Healthy Personal Boundaries, https://www.youtube.com/watch?v=pC5FtPX6Ngg, or another age-appropriate video
b. Discuss as a class the important concerts in the video and how students can apply them to their own lives.

Activity (15 minutes):

a. Divide the class into small groups (three to four per group).
b. Hand out scenario slips with examples of online conversations.
c. Have students discuss if each scenario represents safe or unsafe behavior.
d. After discussing, ask each group to share their conclusions and justify their thinking.
e. Offer feedback and suggestions as needed.

Conclusion (5 minutes):

a. Ask students to name some things they can do if they feel uncomfortable with someone online. Guide students toward answers like blocking/reporting users, not sharing personal information, and telling a trusted adult.
b. Reinforce the importance of listening to their instincts and reporting any suspicious behavior.

Assessment:

a. An informal assessment can be taken based on student participation in discussions and group activity.

Scenarios for Red Flag Activity:

1. An online friend you have known for 2 weeks starts asking for your phone number to make it easier to keep in touch.
2. A new online friend immediately asks about where you go to school and where you live.
3. Someone you follow on social media compliments you on a photo and asks for more pictures.
4. A gamer you met in an online game offers to buy you virtual items if you video call them.
5. A classmate connects with you online, and they share a lot about their interests but do not ask you any personal questions.
6. An online acquaintance says they "trust you" after only chatting for a few days and insists that you not tell anyone about your friendship.
7. A friend from a school club adds you on social media and shares some funny memes. They do not ask for any personal information.
8. A new online friend tells you they feel "really close" to you and wants to meet up in person right away.
9. Someone you met on social media keeps messaging you, even when you do not respond, and gets upset if you do not reply quickly.
10. A friend you know from school sends you a message to join a new group chat with other friends.

Answer Key for Red Flag Scenarios:

1. An online friend you have known for 2 weeks starts asking for your phone number to make it easier to keep in touch.
    a. Unsafe: Asking for personal contact information early on can be a red flag, especially if you have not established trust.
2. A new online friend immediately asks about where you go to school and where you live.
    a. Unsafe: Pressing for specific personal information right away is suspicious and can be used to locate you in real life.
3. Someone you follow on social media compliments you on a photo and asks for more pictures.
    a. Unsafe: Requesting photos is often inappropriate and can indicate grooming behaviors.
4. A gamer you met in an online game offers to buy you virtual items if you video call them.
    a. Unsafe: This is a form of bribery and manipulation to encourage sharing more personal information.
5. A classmate connects with you online, and they share a lot about their interests but do not ask personal questions.
    a. Safe: The classmate keeps the conversation light and respects boundaries, typical of a safe interaction.
6. An online acquaintance says they "trust you" after only chatting for a few days and insists that you do not tell anyone about your friendship.
    a. Unsafe: Rapid declarations of trust and a request for secrecy are often red flags.
7. A friend from a school club adds you on social media and shares some funny memes. They do not ask for any personal information.
    a. Safe: Sharing harmless content without personal questions indicates a respectful approach to online friendship.
8. A new online friend tells you they feel "really close" to you and wants to meet up in person right away.
    a. Unsafe: Rushing a relationship and pushing to meet in real life quickly are major red flags.
9. Someone you met on social media keeps messaging you, even when you do not respond, and gets upset if you do not reply quickly.
    a. Unsafe: Excessive messaging and reactions to unresponsiveness are controlling behaviors that indicate a lack of respect for boundaries.
10. A friend you know from school sends you a message to join a new group chat with other friends.
    a. Safe: Including you in group conversations with mutual friends and no request for private or personal information is safe.

Notes

1 Rogers-Nelson, K., January 18, 2018, "'Stranger Danger' is Over – Here's What Parents Are Teaching Their Kids Instead," https://www.sheknows.com/parenting/articles/1137790/stranger-danger-is-over-tricky-people/, retrieved October 14, 2024.

2 (n.a.), (n.d.), "Online Safety for Pre-Teens (11–13)," https://www.internetmatters.org/advice/11-13/, retrieved October 14, 2024.

3 Shutterstock Illustration ID: 1190867332, Figure 3.1, October 30, 2024, used under CRC License.

4 (n.a.), February 14, 2024, "About Child Sexual Abuse," https://www.cdc.gov/child-abuse-neglect/about/about-child-sexual-abuse.html, retrieved October 14, 2024.

5 (n.a.), (n.d.), "Planet Puberty, Identifying Safe People," https://www.planetpuberty.org.au/keeping-safe/personal-safety/identifying-safe-people/, retrieved October 14, 2024.

6 Darkness to Light, April 3, 2020, "How to Be a Safe Adult," https://www.d2l.org/how-to-be-a-safe-adult/, retrieved October 14, 2024.

7 (n.a.), (n.d.), "What to Do If Your Child Is Talking to an Unsafe Person," https://www.d2l.org/how-to-be-a-safe-adult/, retrieved October 23, 2024.

8 (n.a.), (n.d.), "Electronic Tip Form," https://tips.fbi.gov/home, retrieved October 14, 2024.

9 Microsoft, (n.d.), "The Dangers of Oversharing," https://support.microsoft.com/en-us/topic/the-dangers-of-oversharing-79330a32-4ee1-433a-812e-fe4bb3d34511, retrieved October 30, 2024.

10 (n.a.), (n.d.), "The Wayback Machine," https://wayback-api.archive.org/, retrieved June 25, 2024.

11 (n.a.), (n.d.), "Internet Archive: About IA," https://archive.org/about/, retrieved June 25, 2024.

12 (n.a.), (n.d.), "Doxing Definition, What Is Doxing? What Does It Mean to Dox Someone? Fortinet,"https://www.fortinet.com/resources/cyberglossary/doxing#:~:text=The%20word%20%E2%80%9Cdoxing%E2%80%9D%20(also,other%20exploitation%20of%20targeted%20individuals, retrieved June 5, 2024.

13 August 14, 2024, Department of Homeland Security, Digital Safety Series: Know the Threats, https://www.youtube.com/watch?v=E2z9ILAd_tM, retrieved October 30, 2024.

14 Reiff, N., September 29, 2023, "10 Biggest Telecommunication (Telecom) Companies," https://www.investopedia.com/articles/markets/030216/worlds-top-10-telecommunications-companies.asp, retrieved June 6, 2024.

15 Digital Parenting Team, February 8, 2022, "Gaming: Can you Keep Your Kids Safe?" https://www.vodafone.co.uk/newscentre/features/gaming-can-you-keep-your-kids-safe/, retrieved June 6, 2024.

16 Shutterstock, 2024, Figure 3.2, Mystery Person, Shutterstock Stock Vector ID: Stock Photo ID: 2215866177, used under CRC License, retrieved October 30, 2024.

17 Sweeney, B. "It's Not a Game: FBI New York PSA," https://www.fbi.gov/video-repository/its-not-a-game-psa-fbi-new-york-062921.mp4/view, retrieved June 24, 2024.

18 (n.a.), (n.d.), "Financially Motivated Sextortion" https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/sextortion/financially-motivated-sextortion, retrieved June 10, 2024.

19 Vaughan, Emma Henderson, April 15, 2024, "NCMEC Releases New Sextortion Data," https://www.missingkids.org/blog/2024/ncmec-releases-new-sextortion-data, retrieved June 10, 2024.

20 Vaughan, E., April 15, 2024, Figure 3.3, "Financial Sextortion Reports Received from the Public and Electronic Service Providers, Broken Down by Month, Blog," National Center for Missing & Exploited Children (NCMEC), www.missingkids.org/blog/2024/ncmec-releases-new-sextortion-data, used with permission Ann A. Park, Director, Legal Affairs, National Center for Missing & Exploited Children, retrieved October 30, 2024.

21 Angelini, Giorgio and Arthur Jones, Producers, April 5, 2024, “The Antisocial Network: Memes to Mayhem,” www.imdb.com/title/tt31189868/ distributed by Netflix, accessed October 14, 2024.

22 Ofcom, November 29, 2017, “Children and Parents: Media Use and Attitudes Report,” Ofcom, www.ofcom.org.uk/data/assets/pdffile/0020/108182/children-parents-media-use-attitudes-2017.pdf, retrieved June 27, 2024.

23 Fowler, G.A., Washington Post, June 9, 2022, “Your Kids Apps Are Spying on Them,” Apps Violate Kids’ Privacy on a Massive Scale – The Washington Post, https://www.washingtonpost.com/technology/2022/06/09/apps-kids-privacy/, retrieved October 14, 2024.

24 Pasqualotto, Angela, January 17, 2022, “Improving Reading Skills through Action Video Games,” https://www.sciencedaily.com/releases/2022/01/220117115113.htm, retrieved June 6, 2024.

25 https://CommonSense.org, retrieved October 14, 2024.

26 (n.a.), March 5, 2024, “Policies and Procedures for Mandated Reporting,” https://rems.ed.gov/ASM_Chapter2_Reporting.aspx?AspxAutoDetectCookieSupport=1, retrieved October 14, 2024.

27 (n.a.), April 2024, “Preventing Suicide: Suicide Prevention Fact Sheet,” https://www.cdc.gov/suicide/pdf/NCIPC-Suicide-FactSheet-508_FINAL.pdf, retrieved October 30, 2024.

28 Centers for Disease Control and Prevention, National Center for Health Statistics. National Vital Statistics System, Mortality 2018–2022 on CDC WONDER Online Database, released in 2024. Data are from the Multiple Cause of Death Files, 2018–2022, as compiled from data provided by the 57 vital statistics jurisdictions through the Vital Statistics Cooperative Program. Accessed at http://wonder.cdc.gov/ucd-icd10-expanded.html, retrieved November 2, 2024.

29 May 23, 2023, “Surgeon General Issues New Advisory about Effects Social Media Use Has on Youth Mental Health,” Social Media and Youth Mental Health, retrieved November 6, 2024.

30 June 17, 2024, “Surgeon General Calls for Social Media Warning Labels Amid Teen Mental Health Crisis,” Surgeon General calls for social media warning labels amid teen mental health crisis | PBS News, retrieved November 6, 2024.

31 (n.a.), (n.d.), “Electronic Tip Form,” https://tips.fbi.gov/home, retrieved October 14, 2024.

4

FROM AWARENESS TO ACTION

Inspiring Stewardship in a Digital Age

Introduction

Generally, people will agree that the most valuable asset in any organization (public, private, governmental, or academic) is the people, without whom organizations would not function. Equally, almost everyone will agree that the second most important asset in any organization is the operational data, without which most organizations would cease to exist.

Although some may argue, and convincingly so, that given the data-dependent, digitally driven society in which we live and work, these may (with some conjecture) be reversed.

Data is an asset, a valuable commodity that fuels our digital economy. As such, that data eventually requires safekeeping, regardless of ownership, form, importance, or use. Evoking the emerging dominance of cyber stewardship as an essential requirement of our evolving digital economy and its dependent digital society.

This chapter addresses how the relationship between learned leadership skills (discussed in Chapter 1), applying proactive cyber safety practices (discussed in Chapter 2), and embracing the philosophies of cyber stewardship empower students to be good digital citizens and forge a safer online future.

Stewardship

Stewardship is found in many segments of society today, generally defined as the responsible management and care of resources, people, or systems, with an emphasis on sustainability, accountability, and long-term well-being. It involves the ethical and mindful use of resources (natural, financial, human, etc.) to ensure they are maintained or enhanced for future generations.

The concept of stewardship implies acting with a sense of duty or guardianship, often prioritizing the collective good over personal or immediate gains, and is applicable across various sectors, including environmental, corporate, social, and ethical domains (see Figure 4.1).

DOI: 10.1201/9781003466376-4

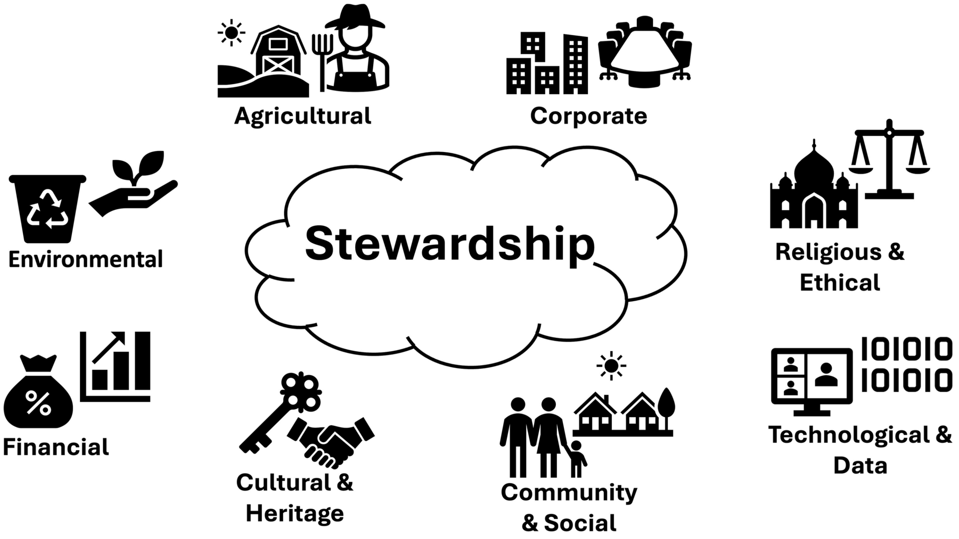


Figure 4.1 Eight types of stewardship.[1]

Fundamentally, stewardship is about the responsible management and care of resources to benefit both present and future generations. Stewardship can be found throughout society in various segments such as environmental stewardship, financial stewardship, organizational stewardship, and more recently, cultural and digital stewardship (see Table 4.1).

Table 4.1 Stewardship Types

SAMPLING OF STEWARDSHIP TYPES	
TYPE	DEFINITION
Biblical	Emphasis is on the proper management and utilization of all resources given to all people.
Community	Management and development of community resources and services.
Conservation stewardship	Use and protection of resources in the natural environment, maintaining land resources to sustain use.
Corporate social responsibility (CSR)	Understand that CSR includes (but is not limited to) corporations being economically responsible, improving labor practices, embracing fair trade, mitigating environmental damage, giving back to the community, and increasing employee satisfaction, and why it is good for business.
Cultural	Responsible management and protection of cultural resources, traditions, and practices within Indigenous communities. This concept emphasizes the importance of maintaining cultural heritage and ensuring that Indigenous knowledge is passed down through generations.[2]
Environmental	Stewardship involves taking care of natural resources such as land, water, and biodiversity to ensure their sustainable use and conservation for future generations. This may include practices such as conservation, sustainable agriculture, and pollution reduction.
Ethical	Ethics is the collection of values, morals, judgments, norms, and standards, which provides a framework for behavior.
Financial	The responsible management of financial resources, whether it be personal finances, corporate finances, or funds belonging to an organization or institution. It involves making sound financial decisions, managing budgets effectively, and ensuring transparency and accountability in financial transactions.

Generation Alpha: Pioneers of Environmental Stewardship

Generation Alpha is even more environmentally aware than Generation Z as they have grown up in a time when environmental issues are more pressing and more in the public consciousness. They are more understanding of climate change and the effect it is having on our world, so much so that many of them are actively taking steps to reduce their carbon footprint and advocate for policies to address environmental issues.

They are also more likely to make purchasing decisions based on a company's environmental practices. As a result, companies are increasingly recognizing the importance of sustainable practices to appeal to this generation of consumers. Overall, Generation Alpha is shaping up to be a generation that prioritizes environmental concerns in their personal and professional lives.[3]

Students are learning to navigate additional levels of responsibility and understand how to act in a responsible role. Responsibility extends to themselves, their classmates, the adults around them, and their community. Parenting Montana sites; research confirms that children are developing cause-and-effect thinking. This directly impacts their capacity to take responsibility for their actions. Once they understand how their actions and decisions affect not only themselves but those around them, they will approach even the smallest things they do in their day with a sense of responsibility and pride.

Teaching Tip

Parenting Montana recommends considering the five-step process to help foster responsibility and make good choices.

1. Get students thinking by getting their input. Ask open-ended questions to prompt thinking.
2. Teach new skills by interactive modeling. Learning new skills and behaviors requires modeling, practice, support, and recognition.
3. Practice growing skills and developing habits. Daily routines are opportunities to practice.
4. Support the child's development and success. Offer support when needed by reteaching, monitoring, coaching, and, when appropriate, applying logical consequences.
5. Recognize effort and quality to foster motivation. Your praise and encouragement are their sweetest reward.[4]

Within organizations, stewardship refers to the responsible management of the organization's resources, including its human capital, physical assets, and reputation. This involves promoting ethical behavior, fostering a culture of accountability, and ensuring that resources are used efficiently to achieve the organization's mission and goals.

How Do We Foster Stewardship Among Teens?

Technology is embedded in our teens' daily routines. They are not hesitant or afraid of where it may take them. Teachers and adults have a responsibility to help them be good stewards of what has been entrusted to them.

The National Science and Teaching Association's Environmental Education Professional Development Institute (EEPDI) emphasizes pathways to integrating next-generation practices with environmental stewardship for informed, responsible action on behalf of the environment and future generations.[5]

The EEPDI Focus emphasizes the integration of *Next Generation Science Standards* (NGSS) practices through student-centered stewardship projects, which offer an excellent means to get students involved in science, increase their critical thinking, and motivate action on environmental issues that are meaningful to the students. One goal was to engage students in "real" local environmental issues by getting them outdoors working in collaborative groups.

The National Science Teaching Association (NSTA) concludes that you, too, like the teachers involved in the EEPDI, can incorporate the *NGSS* Science Practices into your student-driven stewardship projects. These activities can be adapted to students' abilities. The project teachers found helpful also seek cross-disciplinary (e.g., math teachers) collaboration at their school, as well as recruit community expertise outside of their schools.

Science and engineering practices were integrated as students asked questions, planned and carried out their investigation, analyzed and interpreted data, and communicated information. Since repeated exposure is required over many years to deeply understand the disciplinary core ideas and crosscutting concepts and to build students' proficiency with the practices, it is proposed that repeated, varied stewardship projects provide an excellent opportunity for three-dimensional learning.

According to Lesley University's science faculty,[6] the following suggestions are a sampling of ways to encourage being good stewards of the earth. To achieve the right age-appropriate and interest level, adapt the suggestions as needed.

1. Allow Children Unfettered Time in the Natural World: This means not organized sports or adult-directed activities, but lengthy time to explore, play, and invent. It might take the form of building a fort from found objects, damming a stream, or collecting natural objects like shells, rocks, or acorns. These moments in nature are recalled later, as adults, in vivid descriptions.
2. Be a Mentor: Rachel Carson, in her 1956 article entitled "A Sense of Wonder," implored adults to find one child to mentor in the workings of the natural world. Whether parent, grandparent, or other relative or friend, most adult conservationists can point to those people in their lives who had a significant influence on them.

   Create opportunities for children to have experiences with the more-than-human world. Volunteering at a wildlife rehabilitation center, snorkeling on a vacation, or simply walking in nature and having a surprise encounter with local species are all important ways children can encounter the species that share their home. Speak of them as friends and talk about how they are connected to humans.

3. Study the Local Bioregion: Guide children to understand the area they live in for instance, where their water comes from and where it goes once it leaves their home or school; what plants are native or non-native, wild or cultivated; what animals share their home with them; how people make a living from the earth's resources; and what natural wonders; ponds or streams, marshes, hills, and so on; are nearby.
4. Engage Children in Real-Life Actions: Whether it is planting trees, creating a garden, pulling invasive species, or picking up garbage, begin the stewardship mindset.
5. Get to Know Your State or National Parks: If you are lucky enough to live near a protected area, visit. These parks are protected for a reason and offer wonderful hiking opportunities, exploring, and experiencing the sounds, smells, and excitement of unfamiliar natural environments.

Consider ways to incorporate outdoor activities in your day. If this is incorporated early in life, tweens embrace being outside. If it has not been a part of the routine, and maybe there has been more screen time than outside time, it will have to be intentional.

- Schedule time outdoors so it becomes part of the routine.
- Ensure outside school activities during the day. When permitted, move activities outside.
- Create outdoor group activities that have a purpose. Teens need to understand the why behind what they are doing.
- After the outdoor activity, create a discussion about what they liked, do they want to repeat the activity, and what they would like to do next time.

As a mentor and role model, show that it is worth the effort!

Technological and Data Stewardship — Issues for Student Discussion

When discussing technological and data stewardship with middle school students, it's essential to highlight the role they can play in protecting personal data and understanding how technology impacts their lives.

Table 4.2 identifies key issues related to technological and data stewardship, with examples that educators may wish to discuss with students to assist them in improving their online cyber safety presence.

Table 4.2 Key Issues Related to Technological and Data Stewardship

CYBER SAFETY AREA OF CONCERN	ISSUE	EXAMPLE FOR STUDENTS
Data privacy	The protection of personal information, such as passwords, social media posts, or location data.	Imagine if someone you didn't know could see every message you've ever sent, or track where you go every day just because your privacy settings on social media were too open.
Password security	Using weak or easily guessable passwords makes it easier for hackers to access your accounts.	If your password is "123456" or "password," someone could easily guess it and take over your gaming or social media account. Use hardened passwords or better yet, use passphrases to mitigate unknown and unauthorized persons from accessing your personal and private information.
Phishing and scams	Hackers trick people into giving away personal information through fake emails, texts, or websites.	You might get an email or message saying you've won a new phone or a gaming console, but it asks for your personal details or passwords. BE ALERT. BE CYBER SAFE!!
Cyberbullying and digital etiquette	Using technology to bully, harass, or spread false information about others.	Imagine someone spreading rumors or making mean comments about you in a group chat, thinking no one will ever find out.
Social engineering	Manipulating people into giving away confidential information by pretending to be someone trustworthy.	Imagine getting a message from someone pretending to be your friend, asking for your gaming account login because they "forgot theirs."
Digital footprint	Everything you do online, from what you post to the sites you visit, leaves a digital trail that can be permanent.	Even if you delete a post, it can still be saved or screenshot by others. Be smart, be prudent. THINK before you post … the world IS watching.
Software updates and patches	Failing to update your devices and apps can leave them vulnerable to hackers who exploit weaknesses in older versions.	Think of it like upgrading your favorite game — if you don't update it, you can miss out on new features and security fixes.
Malware and viruses	Downloading files, apps, or clicking on unknown links can infect devices with malicious software that can steal information or cause damage.	Imagine downloading what looks like a cool game mod, but instead of helping you win, it puts a virus on your computer that steals your passwords. Investigate fully first-time or unknown sites. Know before you go … don't download files without knowing where they come from, who sent them or what they are. Be cyber smart!!
Oversharing on social media	Posting too much personal information online can make it easy for cybercriminals to steal your identity or manipulate you.	If you post your birthday, school name, and favorite hobby or online game, it's like giving a stranger all the clues to guess your online passwords or find you.
Using public Wi-Fi safely	Public Wi-Fi networks (like in coffee shops or malls) can be less secure, and hackers might intercept your data.	You might think it's cool to use free Wi-Fi at a café to play games or check your social media, but without considering using an encrypted, secure connection, a hacker could steal your login info or other important credentials.
Piracy and illegal downloads	Downloading movies, music, or games illegally can expose you to malware and violate copyright laws.	You might find a site offering free downloads of a popular new movie, but by using it, you could download malware that harms your device.

Cyber Stewardship

Cyber stewardship and data stewardship are related concepts that involve managing and protecting data and cyberspace, respectively.

The idea is that cyberspace is a commons that belongs to no one, but that people must protect and manage it. Motivations for cyber stewardship can include a sense of duty, a desire to reciprocate for the benefits of cyberspace, or a utopian vision for a global society.[7]

Cyber stewardship in general refers to the responsible and ethical management of digital spaces, technologies, and data. It encompasses the safeguarding of information (data privacy and security: Companies and governments are expected to be responsible stewards of individuals' personal data), ensuring privacy and security in the digital age, the ethical use of digital resources (ethical artificial intelligence (AI) and algorithm development: With the rise of AI, organizations are urged to be stewards of fair, unbiased, and transparent AI systems), and the protection of individual privacy and rights within cyberspace. Cyber stewardship focuses on ensuring that digital environments are secure, inclusive, and sustainable for current and future users (sustainable technology development: This involves the creation and implementation of technologies that are not only efficient but also minimize environmental impacts.)

What Does It Mean to Be a "Steward of Cyberspace"?

A steward of cyberspace is an individual or organization that takes responsibility for the ethical management, protection, and governance of digital environments and the information within them. This role involves the following:

- Safeguarding Digital Infrastructure: Ensuring that networks, systems, and data are secure from unauthorized access, breaches, and other cybersecurity threats.
- Promoting Ethical Behavior Online: Encouraging responsible, respectful interactions and ensuring that digital technologies are used in ways that benefit society and uphold human rights.
- Advocating for Digital Literacy and Inclusion: Supporting education and access to technology to ensure equitable participation in the digital world, while promoting understanding of data privacy, digital citizenship, and security practices.

What Makes a Cyber Steward?

A cyber steward possesses several key qualities:

- Accountability: They take responsibility for the management and protection of digital assets, ensuring transparency and trust in how data and systems are handled.

- Ethical Leadership: They champion ethical practices in cyberspace, from data privacy to the fair use of technology, balancing innovation with user rights and societal impacts.
- Security Focused: They prioritize cybersecurity measures to protect digital infrastructures from attacks, including the implementation of proper safeguards, encryption, and monitoring.
- Advocacy for Digital Rights: They advocate for the protection of individuals' rights online, such as privacy, freedom of expression, and equitable access to technology.
- Collaboration and Cooperation: They work with others, whether individuals, organizations, or governments, to foster a safe, inclusive, and resilient digital environment. This includes sharing knowledge and resources to address global digital challenges.
- Long-Term Vision: A cyber steward understands the long-term implications of digital actions and policies, working to ensure that digital spaces remain viable and beneficial for future generations.

A cyber steward, therefore, is an ethical leader in the digital space, focusing on security, responsibility, and the well-being of all participants in cyberspace, ensuring a sustainable and safe future for all.

Cyber Stewardship: Practical Application for the Classroom

The following are four activities that educators may wish to incorporate into student class discussions or out-of-class assignments to help reinforce the important concepts of cyber stewardship.

Activity

#1 Stewardship Discussion Questions
(Small Break-Out Groups for Discussion)

1. What does "stewardship" mean?
2. What do you think it means to be a Cyber Steward?
3. Why is it important to keep cyberspace safe for everyone?

After the students have had an opportunity to discuss in small groups, each group responds to the entire class; the educator can summarize, assuring that key points have been emphasized, and explain the idea of Cyber Stewardship as follows:

Cyber Stewards are people who take care of the digital world by protecting information, ensuring online spaces are safe, and encouraging others to act responsibly online.

Cyber Safety means protecting personal information and keeping yourself and others safe from hackers, scams, and cyberbullying.

Activity

#2 Common Cyber Issues Students May Encounter

Dividing students into small groups, present the following cyber issues, assigning one issue to each group:

- Phishing Emails — Fake emails that try to steal your information.
- Weak Passwords — Simple passwords like "12345" or "password" that hackers can easily guess.
- Cyberbullying — Hurting or embarrassing someone through online messages, posts, or videos.

Ask each group to

1. discuss what might happen if someone falls victim to this cyber issue;
2. think of ways they could be Cyber Stewards in this situation. How would they protect themselves and others?

If discussion stalls and the students seem out of ideas or do not know where to go next, the educator may wish to help students "keep the discussion moving" by asking the following:

1. Phishing: What should you do if you receive an email that looks suspicious? How can you help your friends and family spot phishing emails?
2. Weak Passwords: Why is it important to have a strong password? How can you create one?
3. Cyberbullying: If you see cyberbullying happening, how can you act as a Cyber Steward and help stop it?

Activity

#3 Cyber Steward Action Plan

Ask students to imagine they have just been hired as "Cyber Steward Ambassadors" for their school. Their job is to create an Action Plan that will help their classmates stay safe online.

Breaking students into groups, have each group create a Cyber Steward Action Plan using the following structure:

- Title of Plan: (Example: "Stay Safe, Stay Smart Online")
- Issue: Describe the cyber issue they are focusing on (Phishing, Password Security, Cyberbullying).
- Action Steps: List three actions students can take to address this issue and keep themselves and their friends safe.
  - Using phishing as an example, the educator can provide the following "action steps" to foster additional student ideas:
    - Don't click on strange links.
    - Verify the sender of an email before responding.
    - Report suspicious emails to an adult or teacher.

- Why It Matters: A short explanation of why this plan is important for keeping the school's online environment safe.

Each group presents its Cyber Steward Action Plan to the class. Encourage creativity!

Activity

#4 My Digital Footprint and the Planet

Ask students to think about how often they use technology in a day (phones, computers, gaming consoles, etc.) and where they use this technology. (e.g., social media, streaming, online gaming). Write a few examples on the board.

Explain that every time we use these technologies, we consume energy, which has an environmental impact. Briefly talk about how data centers, which store and manage all the content we access online, use large amounts of electricity, contributing to carbon emissions.

Depending on your students' exposure to the terminology and science, you may need to explain what carbon emissions are and why they are an important consideration/issue in environmental stewardship.

Briefly…

> Carbon emissions are the release of carbon dioxide (CO_2) into the air. This happens when we burn things like coal, oil, and gas to create energy—whether it's for driving cars, powering factories, or using electricity at home. CO_2 is one of the gases that trap heat in the Earth's atmosphere, a process called the "greenhouse effect." This can lead to global warming, which is making the Earth hotter over time.
>
> Carbon emissions are important because they contribute to climate change, which can cause problems like rising sea levels, stronger storms, and even harm to plants and animals. Environmental stewardship means taking care of the planet, and one way we can do that is by reducing carbon emissions. By using less energy, choosing renewable energy sources like solar or wind, and being mindful of our habits (such as turning off lights when not in use), we can help slow down climate change and protect the Earth for future generations.

Breaking students into groups, ask students to list on paper all the ways they use technology in a typical day. Examples might include browsing social media, watching YouTube videos, or playing video games.

Then, have them brainstorm ways they could reduce their digital usage in eco-friendly ways (e.g., turning off devices when not in use, downloading music instead of streaming it repeatedly).

Have each group share, with the entire class, one or two habits they could change and discuss how it could help reduce their environmental footprint.

Summarize the group's findings and emphasize that small, mindful changes in digital use can contribute to environmental stewardship. Conclude by encouraging students to try reducing their digital use for the next week. Have them keep a log of what they did to reduce their digital footprint and overall carbon emissions.

Activity

#5 Create a Cyber Stewardship Pledge

As a different out-of-class activity, ask each student to write a cyber stewardship pledge that they would sign and share that pledge with the class.

As a group, have the students identify the most critical pieces of a pledge from all of the individual pledges created. Then, as a class, combine these into an overall class-wide cyber stewardship pledge.

If students need "direction," the educator may offer up the following as an example, however, stressing that it is important for students to craft their own pledge to begin with.

> I, [student name], pledge to be a responsible Cyber Steward. I will protect my personal information, create strong passwords, and help others stay safe online by promoting respect and kindness in all my digital interactions.

Digital Literacy

> Many young people don't know how to engage in productive dialogue across digital spaces and platforms, or how to create media that represents their authentic views, or how to manage their online lives — including their privacy — in a way that is safe and comfortable for them. That's where educators can step in.[8]
>
> *Grace Tatter*

Digital literacy is rooted in one's knowledge of computer and Internet-based skills such as creating and using strong passwords and passphrases, safeguarding one's privacy, recognizing email scams and deepfakes, protecting against identity theft, and promoting the ethical use of technology.

Teaching students digital literacy requires educators with specific knowledge and skills in areas of information technology and security, compared to a broader set of skills required to teach digital citizenship.

The Oregon Department of Education recognizes that as an educator, digital literacy means providing students with skills that are crosscutting across content areas and are important in all areas, including, but not limited to, communication skills, critical thinking, analysis, and evaluation of media (critical media literacy), digital citizenship, etc.[9]

The Oregon Department of Education has created and implemented across school districts the Five Key Components to be considered for digital learning. See Figure 4.2.

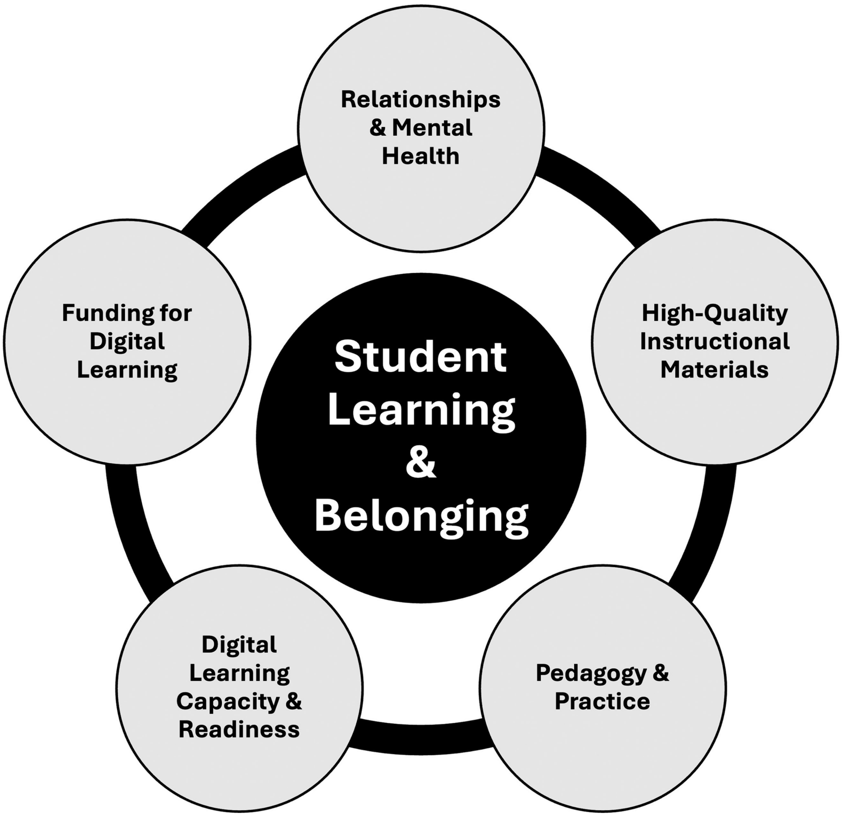

Relationships & Mental Health
High-Quality Instructional Materials
Pedagogy & Practice
Digital Learning Capacity & Readiness
Funding for Digital Learning
Student Learning & Belonging

Figure 4.2 Key components of digital learning.[10]

These five key components, in brief, are as follows:

1. Relationships & Mental Health
    - Create structures to build community.
    - Foster a sense of belonging and safety for each student.
    - Partner with families to create a supportive learning environment.
    - Supporting staff is essential to supporting students.
2. High-Quality Instructional Materials
    - Determine a quality core curriculum.
    - Focus on culturally and linguistically responsive teaching.
3. Pedagogy & Practice
    - Design for purposeful learning.
    - Center in students' lived experiences.
    - Use digital tools and instructional materials to support students' strengths and needs.
    - Ensure regular, timely, and meaningful feedback.
    - Promote engagement, deeper learning, and discourse.

4. Digital Learning Capacity and Readiness
    - Design backward for long-term sustainability and systems-level change.
    - Ensure access to the technology and connectivity needed for learning.
    - Provide device options that meet minimum requirements to access the tools and platforms.
    - Provide training to staff, students, and families about student data privacy and cybersecurity.
5. Funding for Digital Learning
    - Use federal funds to support digital learning efforts.[11]

The Oregon Department of Education's five key components for digital learning encourage building community, fostering belonging, using culturally responsive teaching, and ensuring equitable access to technology.

Empowering Middle School Students through Digital Literacy

Educators can empower their students to greater digital literacy by

- fostering critical thinking skills that allow them to evaluate online information and discern credible sources from misinformation;
- incorporating engaging activities that teach responsible online behavior, helping students understand the impact of their digital footprint;
- encouraging collaboration through digital platforms to enhance communication skills while teaching the importance of digital etiquette; and
- introducing students to creative and ethical uses of technology, inspiring them to become active participants in their online communities.

Teaching students digital literacy through this approach equips students with the tools they need to navigate their digital and offline world safely, responsibly, and thoughtfully.

Digital literacy goes beyond basic tech skills, incorporating critical thinking, media evaluation, and digital citizenship. Educators play a crucial role in guiding students to safely manage their online and offline presence and engage productively in the digital environment of today's society.

What Is Digital Citizenship?

Defining such a term that will effectively and properly describe an individual in today's constantly evolving, digital society is challenging, to say the least, as there is no one agreed-upon official definition … and that may be OK. As technology evolves and as it takes humanity and society along for the ride, it may be best for the near term that we keep an open mind to how we want to describe and define exactly what being a digital citizen is and how that citizen should behave in a digital world.

Joseph Pratt writes that digital citizenship includes all the rights and responsibilities needed to engage in a digital community in a meaningful and safe way.

Put another way, citizens of a country, state, or city should have certain freedoms (such as the right to a fair trial or freedom of speech). Likewise, they have legal obligations (think jury duty, obeying the law, or pulling over for a policeman) that they must fulfill to be considered "productive members" of their community.

Similar responsibilities apply to one's digital community.

In other words, citizenship in the "real world" is both what you owe to your community and what your community owes to you.

Citizenship in the digital world is the same — what you can expect from your online community and what you can expect to do for your online community.[12]

The National Council of Teachers of English defines digital citizenship as students learning about the rights and responsibilities of people in complex, diverse societies and reflecting on their own ethical choices as they use digital platforms in work, life, and citizenship.[13]

Stated broadly, digital citizenship is the responsible use of technology and applies to anyone who uses computers, the Internet, mobile phones, or other digital devices to engage with society.

Jones and Mitchell write in their paper "Defining and Measuring Youth Digital Citizenship," that instead of instructing youth on the harms of cyberbullying, digital citizenship education efforts helped youth practice using respectful behavior during online disagreements, taking others' perspectives, and supporting individuals who were being targeted negatively, there is a possibility that it could also result in decreased online harassment.

The authors, based on their research, recommend that if digital citizenship education is going to be embraced by schools as the next direction for Internet safety education, then it should follow several critical steps.

Digital citizenship education should

1. be well-defined,
2. incorporate effective educational strategies such as active learning,
3. target specific educational goals and outcomes, and
4. evaluate the impact on intended behavioral outcomes.[14]

Digital citizenship involves understanding ethical behavior, legal obligations, and the reciprocal relationship between individuals and their online communities. Digital citizenship education is essential for fostering responsible and ethical engagement in the digital age.

Merely having access to the Internet does not guarantee that a person is utilizing it efficiently or successfully.

Frameworks for Digital Citizenship

Identifying the skills necessary to become a good digital citizen has been explored by many individuals, industry professionals, psychologists, and academic researchers. It is appropriate within this chapter to provide the reader with a brief examination of two frameworks for becoming a good digital citizen, the first by Moonsun Choi, and the second by Mike Ribble. Depending on the available time and size of the class, these frameworks may be discussed separately in individual class exercises or combined into a single class presentation and discussion session.

Choi's Four Categories of Digital Citizenship

The first framework, as proposed by Moonsun Choi, examines the concept of "digital citizenship" and how it relates to educating citizens for a democratic society in the context of widespread Internet use by presenting four specific categories that provide avenues to becoming a good global digital citizen (see Figure 4.3).

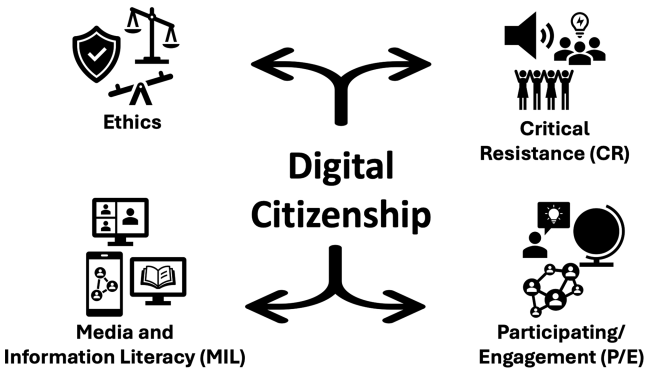

Ethics
Critical Resistance (CR)
Digital Citizenship
Media and Information Literacy (MIL)
Participating/ Engagement (P/E)

Figure 4.3 Choi's four categories of digital citizenship.[15]

Choi's four categories for fostering global digital citizenship are defined as follows:

Digital Citizenship as Ethics Digital citizenship as ethics refers to how Internet users appropriately, safely, ethically, and responsibly engage in Internet working activities.

The concept of digital citizenship has started to integrate such issues as mutual respect, preventing cyberbullying, creating safe communities in an online world, and being aware of community and global responsibilities when using social network sites.

Key components that identify this category include

- ethical use of technology,
- digital awareness, and
- digital responsibilities & rights.

Digital Citizenship as Media and Information Literacy (MIL) Digital citizenship as MIL denotes one's abilities to access, use, create, and evaluate information and communicate online. MIL also embraces the critical analysis process of a wide variety of forms, such as print, audio, video, and multimedia.

Simply having Internet access does not necessarily mean the individual is using the Internet effectively and successfully. MIL also includes "technical skills," which represent an instrumental perspective on literacies and competencies, such as how to use new digital technologies, computers, smartphones, and/or tablet PCs.

Key components that identify this category include

- digital access,
- technical skills, and
- psychological capability.

Digital Citizenship as Participating/Engagement (P/E) Digital citizenship as P/E introduces different types of online engagement, including political, socioeconomic, and cultural participation. For example, from an educational perspective, there is some agreement within the research community that when students learn online etiquette and communication skills, they become good digital citizens.

Key components that identify this category include

- political, economic, and cultural engagement, and
- personalized participation.

Digital Citizenship as Critical Resistance (CR)
Digital citizenship as CR takes more progressive and radical viewpoints than P/E and denotes more critical participation in challenging the status quo and promoting social justice via the Internet. However, the division between P/E and CR is not always clear-cut, as both are related to active, goal-driven participation in virtual communities. CR pursues more creative, innovative, nonlinear, and non-hierarchal forms of participation, potentially leading to a deeper level of digital engagement.

Key components that identify this category include

- critique of the existing power structure and
- political activism.

Implications for Education and the Educator

In teaching digital ethics, students should be taught to take responsibility but more in terms of being productive members of a shared, project-based online community, avoiding activities that might negatively impact both traditional and online communities (such as piracy).

Digital citizenship as MIL can also help educators understand that being informed citizens is not to put something in a search bar and/or just go to Wikipedia to find information. Rather, educators can provide more advanced and higher levels of skills and knowledge regarding how to express ideas and opinions online, evaluate information, and create online content.[16]

Ribble's Nine Elements of Digital Citizenship

Mike Ribble, in his article "Essential Elements of Digital Citizenship," identifies three categories of digital citizenship: respect, educate, and protect, and nine elements within these categories providing a framework to teach the basics of digital citizenship to students.

Ribbie's nine elements of digital citizenship, designed to assist students in navigating online resources, are summarized in Table 4.3.

Ribbie's nine elements of digital citizenship are designed to help students navigate digital environments.

These nine elements of digital citizenship (not a set of rules) can be implemented to guide students to become good digital citizens. They can help parents know how to teach their children about being good digital citizens.

Teaching Tip

Empowering Students through Digital Citizenship: A Fusion of Ribble's and Choi's Frameworks

Using Mike Ribble's and Moonsun Choi's approaches to teaching digital citizenship provides a well-rounded, multidimensional framework that is particularly helpful for middle school educators. Both approaches complement each other by offering a blend of foundational digital skills, ethical behavior, and deeper critical thinking about online participation.

Table 4.3 Ribbie's Nine Elements of Digital Citizenship[17]

CATEGORY	ELEMENT
Respect	• **Digital Access**: Advocating for equal digital rights and access is where digital citizenship starts. • **Digital Etiquette**: Rules and policies aren't enough — we need to teach everyone about appropriate conduct online. • **Digital Law**: It's critical that users understand how to properly use and share each other's digital property.
Educate	• **Digital Communication**: With so many communication options available, students need to learn how to choose the right tools according to their audience and message. • **Digital Literacy**: This involves more than being able to use tools. Digital literacy is about how to find, evaluate and cite digital materials. • **Digital Commerce**: As students make more purchases online, they must understand how to be effective consumers in a digital economy.
Protect	• **Digital Rights and Responsibilities**: Students must understand their basic digital rights to privacy, and freedom of speech. • **Digital Safety and Security**: Digital citizens need to know how to safeguard their information by controlling privacy settings. • **Digital Health and Wellness**: One important aspect of living in a digital world is knowing when to unplug. Students need to make informed decisions about how to prioritize their time and activities online and off. Balance is one of the five competencies of DigCitCommit.

Educators may wish to consider blending the two frameworks in their instructional exercises, as they can be beneficial in teaching middle school students to be good digital citizens:

The following examines how the two frameworks work together to foster digital citizenship and how students can benefit from this fusion.

Comprehensive Framework for Digital Behavior

- Mike Ribble's Approach (Respect, Educate, Protect): Ribble's framework breaks digital citizenship into nine key elements that are organized into three core areas: Respect, Educate, and Protect. For middle school students, this helps provide a clear, actionable structure for understanding the different responsibilities of being a digital citizen.
  - Respect: Teaching students to practice digital etiquette, understand online laws, and advocate for equal access helps students develop respect for others in online communities.
  - Educate: Ribble's focus on digital literacy and communication encourages students to not just be consumers of digital content but critical thinkers who evaluate information and communicate effectively.
  - Protect: Focusing on safety and wellness, Ribble helps students understand the importance of protecting their personal information and knowing when to "unplug" for their mental health.

  For middle school students, these principles give clear guidelines on how to conduct themselves online and offer practical steps for safe and responsible online behavior.
- Moonsun Choi's Approach (Ethics, Media Literacy, Engagement, CR): Choi's analysis brings in broader, more critical perspectives on digital citizenship that go beyond behavior and into understanding the social and political implications of digital engagement.

  Her categories — Ethics, MIL, Participation/Engagement, and CR — challenge students to think about their role in the digital world beyond just personal conduct.
  - Ethics: Encouraging responsible behavior online, Choi's focus on digital ethics helps students understand not only the "how" but also the "why" behind appropriate online behavior.
  - Media Literacy: Choi's emphasis on media literacy helps students critically evaluate information, recognize biases, and avoid misinformation — skills that are crucial for young people growing up in an information-rich digital age.
  - Engagement and CR: By encouraging participation in meaningful online communities and challenging unjust systems (CR), Choi helps middle school students begin to see themselves as agents of change in their digital environments. This can inspire them to use their digital platforms for good, whether through civic engagement, advocacy, or social justice efforts.

Ethical and Safe Use of Technology

- Why Ribble Helps: Ribble's elements, like Digital Law and Digital Safety, ensure that students are educated on how to ethically and legally use technology. This is critical in teaching students about the importance of intellectual property, the proper use of digital tools, and how to safeguard their privacy.
- Why Choi Helps: Choi's approach extends this by not just focusing on individual responsibility but also teaching students to think critically about the broader ethical dimensions of technology use. For example, discussions around digital ethics can help students think about their role in fighting cyberbullying or speaking out against misinformation.

Promoting Critical Thinking and Active Participation

- Ribble's Educational Focus: Ribble's focus on digital literacy and digital communication encourages students to become critical consumers of online content, fostering media literacy skills that allow them to differentiate between reliable and unreliable and disinformation. This also teaches students the value of clear and respectful communication in online environments and how to guard against believing something simply because it appears online without first vetting its source.
- Choi's CR and Participation: Choi goes a step further by encouraging students to engage in CR, where they don't just passively accept digital content but actively engage with it to challenge injustices. This aligns with teaching middle schoolers how to be active participants in their online communities, fostering a sense of empowerment that they can use their voices for social good.

Development of Responsible Digital Habits

- Ribble's Framework Focuses on Balance: Ribble introduces concepts like digital health and wellness, which are essential for teaching students to balance their online activities with offline life. This is especially crucial for middle school students who are experiencing the lure of social media and video games. Teaching them how to unplug, prioritize health, and manage screen time will set the foundation for healthier digital habits.
- Choi's emphasis on media literacy also contributes to healthy digital habits by teaching students how to navigate a complex online world, critically evaluate content, and understand how digital platforms are designed to capture their attention. In the end, teaching students the necessary skills to unplug and to place life wellness ahead of spending more time in virtual environments.

Empowering Students to Use Their Voices for Good

- Ribble's Digital Communication & Commerce: Ribble's approach empowers students to use digital tools effectively, particularly in terms of communication and responsible consumption. This is helpful for middle schoolers as they begin to use online platforms for communication, socializing, and online shopping. Understanding how to communicate appropriately and being aware of their digital footprint encourages responsible digital awareness, participation, and behavior.
- Choi's Focus on Engagement and CR: By emphasizing participation and engagement, Choi's approach helps students feel empowered to take part in online communities and movements. This aspect of digital citizenship is particularly important for middle school students, who are beginning to explore their own identities and can be encouraged to use the Internet to advocate for causes they care about.

Making Digital Citizenship Relevant to 21st-Century Students

- Ribble's Adaptable Structure: Ribble's framework can be adapted across various subjects and grades, which is beneficial for middle school educators who can tailor their lessons on digital citizenship according to specific topics (e.g., addressing cyberbullying in a social studies class or responsible communication in language arts).
- Choi's Broad Perspective: Choi's multidimensional approach helps students relate digital citizenship to real-world issues such as social justice, political activism, and community participation. This broader understanding of citizenship makes the concept more engaging and relevant for middle schoolers, who are beginning to form their social identities.

Using Mike Ribble's practical, foundational approach alongside Moonsun Choi's broader, critical perspective provides educators with a blended robust framework to teach digital citizenship in a way that is accessible, engaging, and transformative for middle school students. Ribble provides the structure for safe and responsible behavior, while Choi challenges students to think critically and engage meaningfully in their digital lives, helping them become well-rounded, empowered digital citizens.

Practical Application: Digital Citizenship Education in the Classroom

It is important that, in teaching digital citizenship, educators focus on teaching students specific social skills. In essence, digital citizenship education should focus on teaching students:

- Respectful behavior skills for engaging with others in both on- and off-line environments;
- Tolerance for others, both in online settings and offline, first-person interactions;

- Importance of involvement in community activities, which refers to behaviors intended to benefit the common good (e.g., environmental restoration projects, working to improve the local community, volunteering with nonprofit organizations, assisting in mitigating the impact of social injustices, solving a community problem).

Educators may wish to incorporate the following activity into a lesson plan where students practice perspective-taking in online disagreements and learn how to demonstrate respectful, supportive actions when witnessing or participating in online disputes.

Activity

Walk in Their Shoes: Online Respect and Perspective-Taking

This activity uses role-play and discussion to help students understand how to approach online disagreements with respect and empathy, even when opinions differ. Through the use of structured scenarios, students will engage in perspective-taking and examine respectful communication strategies.

Scenario Role-Play Approach:

- Divide the class into small groups (three to four students per group).
- Each group will be given one scenario to role-play. Each student in the group will take on a role based on the scenario, representing different perspectives. Example roles: someone who is upset, someone trying to calm things down, and an observer.

Educator:

- Briefly explain the concepts of perspective-taking (understanding someone else's point of view) and respectful, supportive actions (offering kind, constructive feedback rather than attacking or insulting others).
- Discuss common online situations where disagreements occur, such as social media comment threads, gaming communities, or group chats.
- Ask students: "How can you show respect during disagreements online?"
- Have students act out the initial disagreement based on the scenario.
- Periodically pause the role-play and ask each student to share how their character feels and what they think would be a respectful action to take.
- Resume the role-play, but this time, direct students to use respectful and supportive language to navigate the disagreement.

Sample Scenarios:

1. Scenario 1: In an online group chat, two friends argue over a misunderstanding. One feels left out, while the other thinks it's not a big deal.

2. Scenario 2: On a social media post, someone shares a strong opinion about a video game. Another person disagrees and responds with hurtful language.
3. Scenario 3: During a collaborative online project, one student disagrees with the direction another student wants to take, and things get heated.

The educator is encouraged to create additional customized scenarios that are reflective and representative of the students enrolled in the class and of situations that the educator has observed or has previously discussed with students.

Educator (post-activity debrief with students):

- Ask each group to reflect on the following:
  - What helped resolve the disagreement respectfully?
  - How did understanding the other person's perspective change the conversation?
- Encourage students to share examples of when they've seen or participated in disagreements online and how they can apply these skills in real life.
- Provide students with sticky notes or small pieces of paper. Have them write down one way they will practice perspective-taking and showing respect in their next online disagreement.
- Collect and display the notes as a reminder for all students in class.

Learning Takeaways for the Student:

1. Perspective-taking helps you see beyond your emotions and understand others' feelings.
2. Respectful actions don't mean you have to agree with someone but that you respond in a kind and constructive way.
3. Being a good digital citizen means staying calm, supportive, and thoughtful during online disagreements.

With technology and online engagement becoming increasingly integrated into the daily lives of global citizens, the need to develop the skills and knowledge to navigate the digital world is necessary.

> Digital citizenship isn't just about Internet safety. It's also about being responsible and respectful as you navigate through personal and societal digital environments.

From Cyber Stewardship to Digital Citizenship: Fostering Online Responsibility

Cyber stewardship is about taking responsibility for how we use the Internet and protecting our data. It teaches students to be careful with the information they share online, like passwords, personal details, and even the photos or messages they post.

Being a good digital citizen means knowing how to safely interact with others, protecting your privacy, and understanding that what you do online can leave a digital footprint that can last a long time and affect both you and others in positive or negative ways.

Relating cyber stewardship to good digital citizenship may be easier if students are provided with an example.

Ask students to imagine that they have posted a photo online. Explain that cyber stewardship would help them think about who can see the photo, if it's safe to share, and how it might impact their reputation. If they are careful and think before sharing, then they are practicing good digital citizenship. By learning these skills, students can make smarter choices online and help keep the Internet a safe and respectful place for everyone.

Ethics, Leadership, and the Responsible Use of Technology

As society's digital dependency is destined to only increase, leadership and ethical responsibility are crucial components of using current and emerging technologies effectively. As educators guide students through the growing influence of online platforms, it's essential to understand the traits of effective digital leaders and how leadership can manifest in online communities.

The following material is presented as a series of questions designed for the educator to lead student discussions and investigate the importance of collaboration in leadership, the ethical implications of technology, and concepts such as intellectual property, plagiarism, and fair use.

Discussing these questions with students will demonstrate how respecting others' privacy and digital rights is integral to good digital citizenship and how they can leverage technology for collaborative problem-solving while demonstrating leadership qualities.

What Are the Traits of Effective Digital Leaders?

Digital leaders, like most effective leaders, embody qualities such as responsibility, accountability, and empathy. They lead by example, ensuring that their actions promote ethical online behavior.

For example…

> Jacinda Ardern (Former Prime Minister of New Zealand) became a global symbol of empathetic leadership, particularly in crisis management and human services. Her compassionate response during the Christchurch mosque attacks in 2019 was widely praised for uniting the nation and offering support to the Muslim community. Ardern's swift policy action on gun control in the aftermath of the tragedy demonstrated her ability to lead decisively while maintaining sensitivity to human suffering.

> Sundar Pichai, the CEO of Alphabet (Google's parent company), is recognized for his steady leadership and innovative vision in the tech industry. He has spearheaded initiatives related to artificial intelligence, cloud computing, and sustainability, aiming to make technology more accessible and inclusive. A specific example of his effective leadership is his role in pushing Google's efforts toward sustainability. Under his guidance, Google became the first major company to operate fully on renewable energy. Pichai's leadership reflects a balance of ethical considerations, technological innovation, and global impact.

A digital leader is not only a confident decision-maker but also someone who values the opinions and contributions of others in our digital environment. They demonstrate the ability to inspire, engage, and support their peers, fostering a positive and inclusive online environment. Furthermore, these leaders are forward-thinking, continuously seeking to improve their skills and knowledge to better engage the rapidly evolving world of technology.

Teaching Tip

An example to explain this to students is through a class project where a student leads a group assignment on creating a digital presentation. Encourage this student to ensure that every team member contributes equally, helps resolve any disputes, and makes sure that all resources used for the project are cited properly. This in-class reinforcement example is designed to help students understand that digital leadership goes beyond simply managing tasks — it involves collaboration, ethical decision-making, and supporting others.

How Are Students Able to Demonstrate Leadership Skills in Online Communities?

Students can demonstrate leadership skills in online communities by promoting respectful and responsible behavior among their peers. This can be seen when a student steps in to mediate an online disagreement or encourages others to stay positive in online forums. Leadership in online communities often requires the ability to influence others positively and guide discussions in a direction that is productive and inclusive. In addition, it involves making difficult, yet ethical choices when involving peer groups and relationships, such as reporting inappropriate content or ensuring that privacy settings are used effectively to protect themselves and others.

Teaching Tip

Create an online, class-only discussion forum and have students participate by interacting through this discussion forum. Demonstrate to the students that an individual who takes the initiative to moderate the conversation, ensuring that everyone has a chance to speak and that the dialogue remains respectful, is demonstrating leadership. This example reinforces the idea that digital leadership involves guiding others toward constructive interactions and fostering a supportive online environment.

What Is the Importance of Collaboration in Leadership?

Collaboration is an essential part of leadership. A collaborative leadership style that invites and listens to the voices and perspectives of everyone in a group can result in more creative and impactful solutions.[18]

In a digital context, collaboration allows individuals to pool their skills, knowledge, and creativity to solve complex problems. Leaders who understand the value of collaboration tend to be more successful because they recognize that teamwork leads to more innovative and well-rounded solutions. Collaboration also helps distribute the responsibilities of leadership, making it easier for leaders to manage large or complicated projects. This kind of teamwork also teaches leaders to value diverse perspectives and ideas, which is essential in any leadership role.

Using digital collaboration tools (e.g., virtual video conferencing, instant messaging, social media platforms, etc.) helps students acquire critical and essential digital communication skills.

Teaching Tip

One option that may be used to reinforce this concept to students is to assign a group project where each student is responsible for a different aspect of the task. The student leading the group ensures that everyone's contributions are valued and integrated into the final product. This helps students see that leadership is not about doing everything yourself; it's about bringing people together to achieve a common goal.

The Ethical Implications of Technology Use

Technology brings with it a range of ethical considerations, especially concerning privacy, security, and the potential misuse of information (e.g., disinformation, deepfakes, etc.).

Students are directly affected by technology almost every waking moment, whether in or out of the classroom and must be particularly mindful of the ethical implications of their actions. When discussing the implications of their digital actions with students, students must realize that they should not engage in harmful practices like cyberbullying, spreading misinformation, or violating someone's privacy. Teaching students that ethical technology use also involves an awareness that technology should be accessible to all and not prevent the exclusion of individuals from digital platforms due to barriers like cost or lack of Internet access.

Teaching Tip

As an application of this teaching point, discuss with students how using a social media platform involves ethical decisions. For instance, if a student sees a classmate being bullied online, the student, by acting and reporting the post or offering support to her/his classmate, demonstrates an understanding of both empathy and the ethical implications of technology use. This teaches students to consider the broader impact of their actions in the digital world.

How Does Being a Good Digital Citizen Reflect Respecting Others' Privacy and Digital Rights?

Being a good digital citizen involves understanding and respecting the rights and privacy of others online. This means not sharing personal information without consent, being mindful of what is posted, and avoiding behaviors that could harm or infringe upon someone's privacy. Digital citizenship also includes adhering to the rules of online platforms and understanding the potential consequences of misusing these digital environments. By respecting the rights and privacy of others, students learn to contribute to a more respectful online community and a safer digital world.

Teaching Tip

For example, a teacher might explain to students that sharing a classmate's photo online without permission violates that person's privacy and, in some cases, may even be unlawful. By encouraging students to think before they post and to always get consent, educators can help students understand the importance of digital citizenship and respecting others' digital rights.

How Can Students Use Technology for Collaborative Problem-Solving and Demonstrate Leadership Qualities?

Students can use technology to collaborate on projects that solve real-world problems, such as creating digital campaigns for school events or developing presentations on environmental issues. Students who work together using digital tools can share ideas, delegate tasks, and use technology to enhance their projects. Leadership qualities are demonstrated when students take the initiative, motivate their peers, and ensure that the project stays on track while using ethical digital practices.

Teaching Tip

To reinforce this aspect of collaborative leadership, assign a class project where students are separated into teams and are required to work together to create a digital presentation on climate change, for example. Do not assign specific tasks to the individual students in the group, allowing each group to independently and collectively determine leadership roles and group objectives. The student who organizes the team's efforts, assigns tasks, and ensures everyone's contributions are included demonstrates leadership qualities and characteristics. This exercise assists students in understanding how they can use technology not only to solve problems but also to lead and collaborate effectively.

And finally…

Discuss Intellectual Property, Plagiarism, and Fair Use

Discuss with students that maintaining a basic understanding of concepts such as intellectual property (the ownership of ideas, inventions, and creative works), plagiarism (the act of using someone else's work without giving proper credit), and fair use (allowing people to use parts of copyrighted material for specific purposes, such as education or commentary), is essential knowledge for anyone engaging with digital content.

In a digital world, where information is easily accessible, respecting these concepts is critical for maintaining ethical standards.

Teaching Tip

Assign student teams to create individual digital presentations using images or quotes from the Internet. As the teams create their presentation, assist them by showing them how to properly credit the original creators and explain why it's important not to plagiarize. This example will help students to understand that respecting intellectual property is not just a rule but a way to show respect for others' hard work and creativity.

What Does Stewardship Mean to the Teacher's Role?

In the article "The Importance of Stewardship in Leadership" from the Graduate Programs for Educators, the concept of the teacher as a wise steward of leadership in the classroom is examined.[19] Burress believes these are the expected areas of stewardship when serving as an educator leader. Each of these areas is an important factor in becoming an effective steward of educational leadership.

Stewardship of Students

First and foremost, the most important thing we are entrusted with is our students. What does it mean to be a steward for students? Our communities trust us with their students for 180 days a year. However, more importantly, parents trust us with their children! We need to always ask ourselves the following daily questions:

1. Is what we are doing in the best interest of students?
2. Would you entrust your child with our instructors?
3. Are we making an impact on these children's lives?

As educators, we should never take the responsibility of stewardship of other people's children lightly. Education is a calling; being a wise steward of students is a responsibility that is accompanied by passion, enthusiasm, and joy.

Stewardship of Influence

Educators have a remarkable amount of influence over their students, and educational leaders have the same influence over their staff. We are entrusted to use that influence in such a way that our instructional teams can help our students become productive members of society. We have all heard stories of educators telling students that they are not college material or shouldn't do something because they don't have the right skill set.

Words matter, and misusing words is being a poor steward of influence. Look to these daily questions to ensure you are stewarding your influence well:

1. Is my influence helping instructors be more effective?
2. Would I be motivated by my words?
3. How can my influence help shape my staff in a way that builds our school culture?

We need to use our influence to lift our teachers up so that they can do the same for our students. Consciously choose to lead staff down a path of success. Look to the positives — not negatives — of your team and students. Stewardship of influence is a powerful tool, so use it wisely and lead staff to obtainable goals.

Steward of Relationships

Relationships are a fundamental building block of leadership. As leaders, we are entrusted to build and maintain relationships with many stakeholders. First and foremost, we must build relationships with our students. Building professional, meaningful relationships with kids makes the entire educational process easier for all of us. Get to know your students, relate to them, and build them up.

We also must build relationships with our peers and faculty. We are all here for each other and our kids. Let's encourage one another and remember that our weaknesses are others' strengths. Learn from each other and grow.

The wise steward of relationships works with parents. Make contact and share successes so that when a failure happens, you have formed a relationship and can move forward together. Look to these questions as you steward leadership through relationships:

1. What are my weaknesses, and how can my relationship strengthen those weaknesses?
2. Can my strengths help those around me to be better?
3. How can this relationship make me a better leader?

An educational leader can utilize stewardship of relationships in valuable ways. Leaders are most productive when building relationships. It is hard for anyone to be effective without actively pursuing growth in this area. We are not on an island all by ourselves, but we are here for each other and our students.

Burress suggests you may see a higher priority in one area over another, and asks that as the year begins, you reflect upon them and try to strengthen your stewardship as it relates to your students, staff, school, and community.

Burress's final comment is appropriate for teachers and students as it relates well to the chapter's definition of stewardship — Trust in yourself to be a wise steward and remember, the wise steward leaves the things they are entrusted with in better shape than they were given.

Discussion Activity

One approach when talking about stewardship is to talk about it from the perspective of volunteerism. Based on our definition that stewardship is taking care of what has been entrusted to you, discuss with students what volunteering is, how volunteering impacts them and their community, and what "gifts" are offered through volunteering.

- Definitions:
  - Volunteering: to do something, especially for other people or for an organization, willingly and without being forced or paid to do it.[20]
  - Volunteering allows you to connect to your community and make it a better place. Even helping out with the smallest tasks can make a real difference in the lives of people, animals, and organizations in need.[21]
- Ask students to share any stories from their experiences volunteering.
  - How did it make them feel to help?
  - Have they stayed in touch with people they met through their volunteer work?
- Facilitate a discussion about ways to get involved — asking what the students are interested in and what they like to do. Think about ways to volunteer in those areas. Volunteer Match is a great organization to match volunteers with community needs — About Us Page (volunteermatch.org).
- Focus on the sharing aspect and how volunteering is a good way to be a good steward.

There are no right or wrong answers to this exercise, only to encourage discussing the concept of taking care of what we have been given (see Figure 4.4).

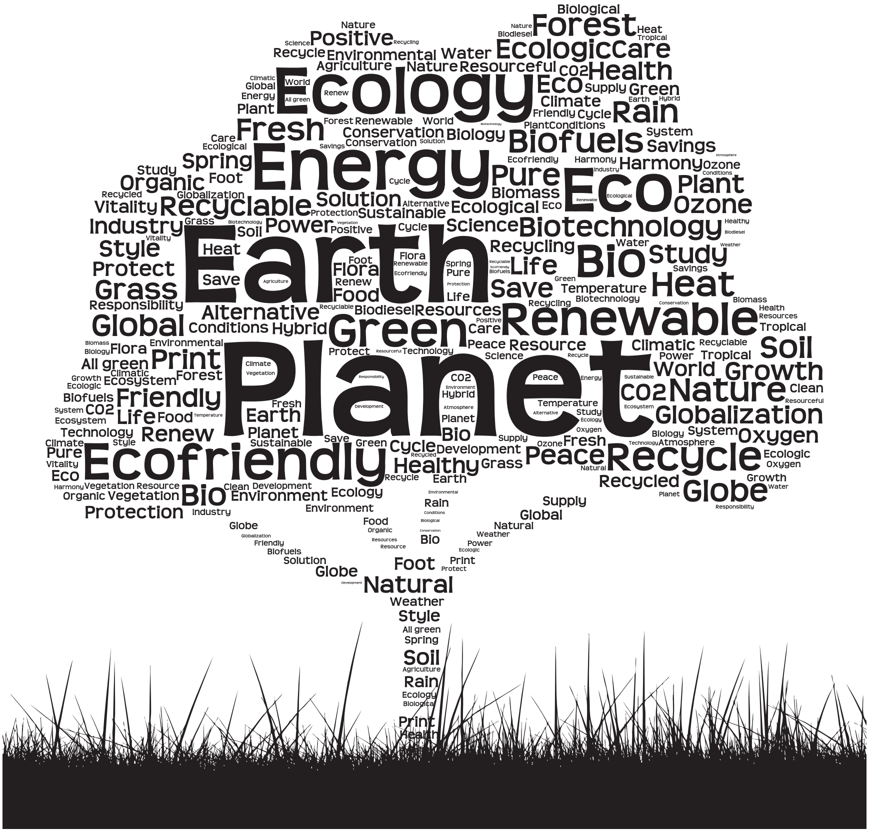

Planet
Earth
Energy
Ecology
Eco
Ecofriendly
Renewable
Green
Recycle
Bio
Biotechnology
Biofuels
Forest
EcologicCare
Health
Heat
Nature
Globalization
Globe
Recyclable
Fresh
Rain
Ozone
Plant
Soil
Growth
Global
Grass
Friendly
Print
Peace
Oxygen
Positive
Harmony
Pure
Study
Save
Life
Organic
Spring
Industry
Style
Protect
Protection
Natural
Foot

Figure 4.4 Planet Earth — environmental sustainability.[22]

Earth Day — Smart Practices

Every year on April 22, Earth Day is celebrated marking the anniversary of the birth of the modern sentimental movement started in 1970.[23] In 1990, Earth Day became an International Day of Observance. Currently, over 192 countries observe Earth Day, and it is the largest secular observance in the world.[24]

Teaching students about Earth Day is vital to future generations understanding the importance of preserving the land on which we live. Each generation bears responsibility for what future generations will inherit. Education is the most powerful catalyst for change. Ideally, after learning about this day's importance, students will be inspired to act, whether that involves planting a tree, recycling at home, or picking up trash at a public park. We only get one Earth, so let's take care of it.[25]

Activity

Not taking care of the earth and the resources it provides is depriving future generations of its bounty. Big steps often start with little steps. If not already familiar with the very popular three Rs related to the environment, this is a good place to start reinforcing the concept of stewardship. Introduce your students to the three Rs — reduce, reuse, and recycle.

- Make this a classroom activity by talking about packaging and waste.
- Discuss how items may be reused. Introduce the idea of repurposing items.
- Recycle what is appropriate as a classroom activity.
- Encourage parents and guardians to participate, as they bring in classroom supplies and treats, and also by extending the three Rs to the home.

Many classrooms already have projects such as growing plants in indoor or outdoor gardens or have incubators for animal propagation, i.e., watching chicks hatch. If you are not already doing this, planting seeds is an easy way to start. Most libraries have free seed libraries. Check to see if your local library provides a free seed program. You may "check out" seeds to plant. It can be a fun and low-cost project.

Activity

Another practical activity is to discuss a global resource and if depleted, the impact this may have on your part of the world. Deforestation is an example.

Discuss what restoration means. The general definition of restoration is the act of bringing something back to a former condition.

This activity may be incorporated into science and geography studies.

- Topic research may include identifying local, country, and continental areas where the landscape or foliage has changed or deteriorated.
- Discuss the impact the change may have on your area. These may include
  - changes to climate impact global warming;
  - water pollution or water depletion;
  - impacts biodiversity, i.e., the number of plants and animals in an area; and
  - changes in greenhouse gases and air pollution.
- Brainstorm ideas to restore these areas.
  - Replace/replant lost native plants.
  - Thin invasive plants.

The need to respect and conserve these resources and ways to accomplish this begins in the classroom.

The peer-reviewed study authored by Eugene Cordone et al., titled "The role of climate change education on individual lifetime carbon emissions," investigated the long-term impact that an intensive one-year university course had on individual carbon emissions by surveying students at least 5 years after having taken the course. Surveys and focus group interviews identify that course graduates have developed a strong personal connection to climate change solutions, and this is realized in their daily behaviors and through their professional careers.

The analysis also demonstrates that if similar education programs were applied at scale, the potential reductions in carbon emissions would be of similar magnitude to other large-scale mitigation strategies, such as rooftop solar or electric vehicles.[26] Imagine if we begin the process of talking about good earth practices at an early age, what the children of today could do tomorrow.

The concepts of respect, care, and environmental stewardship play an important role in the child's online environment as well.

According to Common Sense Media's Census program, on average 13–18-year-olds use about eight and a half hours of screen media per day (8 hours 39 minutes). These figures represent the total amount of screen content young people consume or engage with, adding together the amount of time they spend watching television and online videos, playing video games, using social media, and the like.

These findings on the total amount of screen media used do not mean that young people devote eight and a half hours each day exclusively to screen media, for two reasons. First, they often spend some proportion of time using multiple screens, for example, scrolling social media while watching television, meaning 2 hours of screen content could fit into a single hour of the day.

Second, they often watch or use screen media while they are doing other things, like riding in a car or bus or eating breakfast. It's also important to remember that these time estimates represent the average among all young people and individual use of media varies widely.[27]

Stewardship, Security, and Cyberspace

In his article, "Stewardship, Security, and Cyberspace," James Lewis raises the question of exactly who serves as the true stewards of the Internet. Are the Internet stewards the informal civil, corporate, and technical voices or the technical bodies like the Internet Engineering Task Force, government agencies, or multinational entities such as the Internet Corporation for Assigned Names and Numbers?[28]

Cyber stewardship involves not only technical oversight but also a responsibility toward the public good, which is challenged by conflicting goals between technical bodies, civil organizations, and governments.

As governments seek greater control over cyberspace, tensions arise between informal, community-driven stewardship and the more authoritative approaches of state actors. Governments argue that informal Internet stewardship fails to meet public interests in security and privacy, pushing them to take a more active role in governance.

Raising the timely question, one that makes an excellent learning assignment for students (working independently or in teams)… "Can cyber safety and cyber stewardship coexist?"

Can Cyber Safety and Cyber Stewardship Coexist?

Yes, cyber safety and cyber stewardship can coexist, although achieving a balance between the two requires careful collaboration and shared responsibilities.

Here's how they can work together. Each of the following examples provides a teaching opportunity, allowing students to put theory into application.

Collaboration #1: Setting Rules for Online Behavior

Just like schools have rules to keep students safe, the Internet has rules to protect users from harm such as follows:

- Keep personal information professional and limited.
- Practice safe browsing.
- Be careful what you download.
- Choose strong passwords.
- Make online purchases from secure sites.
- Be careful what you post.
- Be careful who you meet online.
- Keep your antivirus program up to date.

An example for students, once having discussed setting rules for online behavior, is to look at websites that often have terms of service that guide what people can and can't post. These rules help keep the online environment safe (cyber safety) and ensure everyone follows certain standards (cyber stewardship). Table 4.4 provides a representative list of platforms that restrict harmful or inappropriate content, making it safer for users.

Table 4.4 Websites That Restrict Harmful or Inappropriate Content

WEBSITE NAME	DESCRIPTION
Common sense media www.commonsensemedia.org	A review site that rates media (websites, apps, movies, games) for age-appropriateness, helping parents make informed decisions for their children.
Epic! www.getepic.com	A digital library for children, offering thousands of curated books and educational videos that are safe for young readers, widely used in schools.
Google's "Be Internet Awesome" https://beinternetawesome.withgoogle.com	Interactive program teaching kids online safety, privacy, and responsible behavior. Content is educational and promotes safe online habits.
Minecraft education edition https://education.minecraft.net	An educational version of Minecraft that allows creative exploration in a safe environment, with tools for teachers to guide and monitor students' activities.
Scratch https://scratch.mit.edu	A coding platform developed by MIT for children, with strict guidelines and content moderation to ensure shared projects remain safe and appropriate.

Collaboration #2: Protecting Privacy and Data

In many ways, teachers are responsible for protecting students' grades (keeping private information private, adhering to FERPA guidelines,[29] etc.). In the same way, cyber stewards (like website managers or app developers) have a responsibility to protect user data. When schools or apps ask for personal information, they are responsible for keeping that data safe (cyber safety) while also being transparent about how they use it (cyber stewardship). For instance, apps designed for young people often require parental consent and minimize data collection, demonstrating respect for users' privacy.

Collaboration #3: Stop Cyberbullying

Schools, parents, and online platforms work together to prevent cyberbullying. Platforms like Instagram or TikTok have features to report or block abusive content, which helps keep users safe online. This teamwork between the users (students, teachers) and the platforms (stewards) shows how cyber safety and stewardship can work together to create a healthier online environment.

Collaboration #4: Providing Education and Awareness

Just as students are taught about Internet safety, cyber stewards also play a role in educating users about potential risks and responsible online behavior. For example, Google's "Be Internet Awesome" program teaches kids and young adults about staying safe online, helping them understand both safety and responsible use. This type of program shows how cyber safety (protecting kids) and stewardship (teaching responsible behavior) can coexist.

Collaboration #5: Mitigating Hacking and Cyber Threats

As with most schools today, it is standard procedure to have security measures like locks or cameras around and within the school grounds and buildings; the online world has similar security protections. Companies like Apple and Microsoft work on security updates to protect users from hackers. By updating software, they ensure the devices remain safe (cyber safety) while also maintaining users' trust and responsibility (cyber stewardship) to protect the devices we rely on.

These examples show that when organizations, users, and communities all play their parts, it's possible for cyber safety (protection from online harm) and cyber stewardship (responsible and ethical management of cyberspace) to work together, creating a safer, more reliable online world for everyone.

Empowering Youth: Addressing Social Issues through Technology

Students today face a variety of social issues that have a direct impact on their well-being, academic success, and personal development. Among these challenges are bullying, mental health struggles, academic pressure, and issues related to social inclusion. Technology can play a pivotal role in addressing these concerns by offering tools and platforms that support positive interactions, enhance emotional well-being, and create a safer school environment.

Examples can be found in the way that anti-bullying apps and online reporting systems allow students to confidentially report incidents of bullying confidentially, while digital platforms for mental health provide students with access to helpful resources and self-care tools. Educational apps also support personalized learning, helping students manage academic pressures by allowing them to learn at their own pace and seek additional help when needed.

The use of technology to address social issues requires careful consideration and guidance. The potential for cyberbullying, exposure to inappropriate content, and excessive screen time are important risks that need to be managed.

Educators, parents, trusted adults, and school administrators play a crucial role in establishing safe online spaces and setting boundaries for technology use. By promoting digital literacy and online safety, educators (with assistance and support from school administration and parents) can help students understand the responsible use of technology while encouraging them to leverage these tools for positive outcomes.

When used responsibly, technology has the potential to be a powerful ally in supporting students through challenging social issues and creating a safer and more inclusive environment for students, both online and offline. Table 4.5 provides examples of social issues that students face and how these issues may be addressed through oversight and guidance from educators, adults, school administrators, and the use of technology.

Table 4.5 Social Issues and How They Can Be Addressed through Technology

SOCIAL ISSUE	ADDRESSING SOCIAL ISSUES THROUGH TECHNOLOGY
Academic pressure	Study and homework-help apps (like Khan Academy — www.khanacademy.org and Quizlet — www.quizlet.com) provide resources to support learning and reduce stress through interactive learning tools.
Access to reliable news	News literacy websites and apps (like Newsela — www.newsela.com) help students learn to identify credible sources and understand current events in an age-appropriate way.
Body image and self-esteem	Platforms and apps with positive messaging (like Dove's Self-Esteem Project — www.dove.com/us/en/dove-self-esteem-project.html) promote body positivity and offer resources to build self-confidence.
Cyberbullying	Anti-cyberbullying apps and reporting tools on social media platforms can help students report bullying incidents and seek support anonymously.

(*Continued*)

Table 4.5 (*Continued*) Social Issues and How They Can Be Addressed through Technology

SOCIAL ISSUE	ADDRESSING SOCIAL ISSUES THROUGH TECHNOLOGY
Diversity and inclusion	Social media and online forums can connect students with peers from diverse backgrounds, promoting understanding and acceptance.
Environmental awareness	Apps and websites provide educational resources about climate change and ways to reduce waste, allowing students to learn about eco-friendly habits.
Food insecurity awareness	Apps that connect students to local food banks or programs (like Feeding America's app — www.feedingamerica.org) raise awareness and provide resources for those in need.
Mental health awareness	Mental health apps and online platforms (like Calm — www.calm.com or Headspace for Kids — www.headspace.com) offer resources for relaxation, meditation, and mental health education.
Online privacy and safety	Educational games and programs, like Google's "Be Internet Awesome" (https://beinternetawesome.withgoogle.com), teach students about safe online habits and protecting personal information.
Time management	Time-management and productivity apps (like Forest — www.forestapp.cc or Todoist — www.todoist.com) help students develop good habits and balance schoolwork, activities, and free time.

What Is Environmental Stewardship in a Digital Age?

Environmental stewardship in the digital age refers to the responsible management and protection of the environment through the use of technology and digital tools. It involves utilizing technology to promote sustainability, reduce carbon footprints, and raise awareness about environmental issues. Educators can introduce middle school students to this concept by emphasizing the importance of using digital resources to advocate for sustainable practices, such as reducing energy consumption, supporting conservation efforts, and learning about eco-friendly technologies.

To present this topic effectively, educators should encourage students to explore how digital innovations, like apps for recycling and online campaigns for environmental causes, can make a positive impact. Interactive lessons could focus on the relationship between technology use and environmental impact, helping students recognize both the benefits and potential harm of digital devices. By linking everyday digital practices with environmental responsibility, students can understand how their digital choices contribute to a sustainable future.

Conclusion

In a rapidly evolving, digitally dependent society, cyber stewardship emerges as a foundational responsibility, requiring students, educators, and the broader community to approach the use of technology with a sense of duty, responsibility, and foresight. The importance of equipping students with digital literacy know-how, ethical awareness, and proactive behaviors to navigate and contribute positively to their online environments is a critical and essential teaching objective for educators.

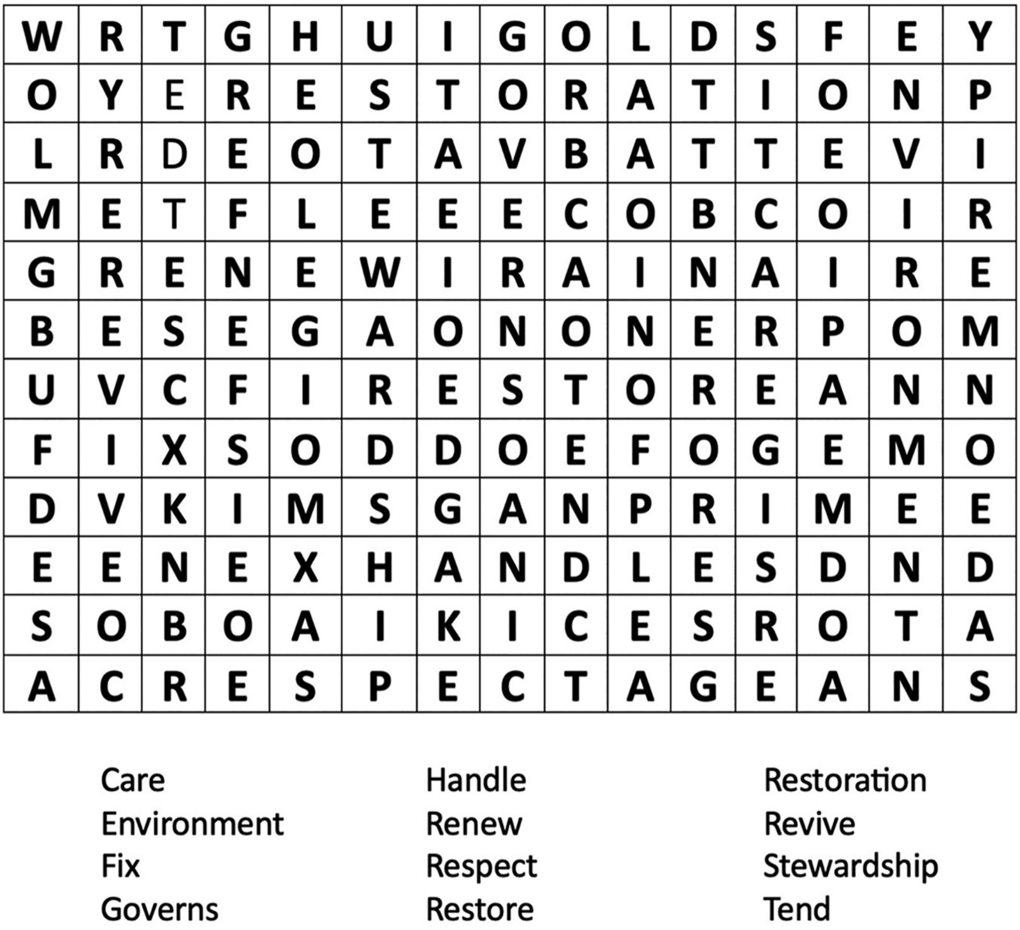
Cyber stewardship, as discussed, extends beyond basic safety, promoting a mindset of long-term accountability for the welfare of digital environments. By developing skills in data protection, responsible information sharing, and respectful online interaction, students are encouraged to think critically about their roles and responsibilities within virtual, digital environments.

Moreover, effective cyber stewardship hinges on a collaborative framework involving students, parents, educators, and technology providers. Together, they can establish and uphold boundaries for safe technology use while encouraging the responsible application of digital tools. As students understand the significance of their digital actions, from safeguarding personal information to engaging in constructive dialogue, they become better prepared to face potential online risks and use technology as a tool for social good.

This holistic approach to cyber stewardship not only protects individual users but also contributes to a safer, more inclusive, and resilient digital society, empowering students to become conscientious leaders of their future digital world (Figures 4.5 and 4.6).

ACTIVITY

Stewardship Word Find Puzzle



W	R	T	G	H	U	I	G	O	L	D	S	F	E	Y
O	Y	E	R	E	S	T	O	R	A	T	I	O	N	P
L	R	D	E	O	T	A	V	B	A	T	T	E	V	I
M	E	T	F	L	E	E	E	C	O	B	C	O	I	R
G	R	E	N	E	W	I	R	A	I	N	A	I	R	E
B	E	S	E	G	A	O	N	O	N	E	R	P	O	M
U	V	C	F	I	R	E	S	T	O	R	E	A	N	N
F	I	X	S	O	D	D	O	E	F	O	G	E	M	O
D	V	K	I	M	S	G	A	N	P	R	I	M	E	E
E	E	N	E	X	H	A	N	D	L	E	S	D	N	D
S	O	B	O	A	I	K	I	C	E	S	R	O	T	A
A	C	R	E	S	P	E	C	T	A	G	E	A	N	S

Care
Environment
Fix
Governs
Handle
Renew
Respect
Restore
Restoration
Revive
Stewardship
Tend

Figure 4.5 Stewardship word find puzzle.[30]

Stewardship Word Find Solution

W	R	T	G	H	U	I	**G**	O	L	D	S	F	**E**	Y
O	Y	E	**R**	**E**	**S**	**T**	**O**	**R**	**A**	**T**	**I**	**O**	**N**	P
L	R	D	E	O	**T**	A	**V**	B	A	T	T	E	**V**	I
M	E	T	F	L	**E**	E	**E**	C	O	B	**C**	O	**I**	R
G	**R**	**E**	**N**	**E**	**W**	I	**R**	A	I	N	**A**	I	**R**	E
B	**E**	S	E	G	**A**	O	**N**	O	N	E	**R**	P	**O**	M
U	**V**	C	F	I	**R**	**E**	**S**	**T**	**O**	**R**	**E**	A	**N**	N
F	**I**	**X**	S	O	**D**	D	O	**E**	F	O	G	E	**M**	O
D	**V**	K	I	M	**S**	G	A	**N**	P	R	I	M	**E**	E
E	**E**	N	E	X	**H**	**A**	**N**	**D**	**L**	**E**	S	D	**N**	D
S	O	B	O	A	**I**	K	I	C	E	S	R	O	**T**	A
A	C	**R**	**E**	**S**	**P**	**E**	**C**	**T**	A	G	E	A	N	S

Figure 4.6 Stewardship word find puzzle — solution.[31]

LESSON PLANS

Grades 7 and 8

TOC Title: G7 and G8 Stewardship

Lesson Title: Stewardship
Grade Level: 7 and 8
Duration: 45 minutes

Objective:

- The students will understand the concept of energy conservation.
- The students will learn how to understand energy use and ways to manage and conserve use.

Suggested Materials:

- Video on responsible energy conservation. Suggestion: *Teaching Kids to Conserve Energy at Home: Resources for K—12 teachers and parents* (youtube.com) (11 minutes 2 seconds), or a similar age-appropriate video covering energy conservation.

Recommendation:

- Teacher preview of video before use to assess appropriate with class.
- Video includes other websites to help explain energy conservation to students and access free resources.

Procedure

Introduction (20 minutes):

a. Discuss the concept of energy stewardship with the class.
b. Show suggested video or another age-appropriate energy conservation video.

Activity (10 minutes):

a. Divide the class into small groups (three to four students per group).
b. Ask groups to discuss how they would act as good energy stewards.

Activity — Optional (10 minutes):

a. Demonstrate and use the Interactive energy use link in the video by inserting information and generate personalized use score.
b. Review the explanation via the video website link and review ways to improve the score.

Conclusion (5 minutes):

a. Summarize the importance of energy stewardship.
b. Encourage students to share what they learned with family and friends.

Homework (Optional as Parental/Guardian Consent Is Required for Site Sign-up):

1. Personalized page upon sign-up for tracking commitments and tracking; rebates on products; see environmental footprint. (Completed at home as sign-up is required.)
2. Energy yardstick kids can use with parents at home.
3. Track use and changes over a 30-day period.
4. Discuss in a follow-up class session.

As an alternative to the students using the site and yardstick, where information needs to be entered, the leader may consider using a personal address (which does not need to be shared with the class) and enter "sample" information for review and discussion.

Assessment:

a. An informal assessment can be made based on each student's participation and contribution to class discussions and group activity.
b. Homework assignment for those able to complete it.

Grade 7

TOC Title: G7 Stewardship
Lesson Title: Stewardship
Grade Level: 7
Duration: 45 minutes

Objective:

- The students will understand the concept of digital stewardship.
- The students will be able to practice responsible online behavior.

Suggested Materials:

- Whiteboard/chalkboard.
- Markers.
- Printed scenarios for activity (provided below).
- Short video related to the topic. Suggestion: *Teen Voices: Oversharing and Your Digital Footprint*, https://www.youtube.com/watch?v=ottnH427Fr8&t=32s (3 minutes 34 seconds), or a similar age-appropriate video

Procedure

Introduction to Digital Stewardship (10 minutes):

a. Whole Group Discussion: Ask the class what it means to take care of something. Discuss stewardship in a general sense.
b. Define Digital Stewardship: Explain that digital stewardship is about taking responsibility for our online actions, respecting others, and keeping ourselves safe online. This includes handling information carefully, being thoughtful about what we share, and respecting other people's content and privacy.
c. Examples: Give relatable examples of digital stewardship, such as keeping passwords safe, not sharing someone else's private messages, and thinking twice before posting or sharing content.

Discussion and Video on Responsible Online Behavior (10 minutes):

a. Show a short video that illustrates responsible online behavior, digital footprints, or respect online. Suggestion: *Teen Voices: Oversharing and Your Digital Footprint*, or a similar age-appropriate video.
b. Ask students questions such as
    - "Why is it important to be careful about what we post online?"
    - "How do our online actions affect others?"
    - "What are some ways we can show respect to others online?"

Activity: The Stewardship Scenario Game (20 minutes):

a. Divide students into small groups (three to four students per group).
b. Hand each group a set of index cards or slips of paper each with a different online scenario (provided below).
c. Groups will discuss the scenario and come up with a solution based on digital stewardship principles.
d. Have each group share their scenario and solution with the class. Discuss as a group whether the solution shows good digital stewardship and suggest any improvements if needed.

Conclusion (5 minutes):

a. Ask students to share one thing they learned about digital stewardship or one way they'll change how they act online.
b. Summarize the importance of being mindful online and how digital stewardship helps create a safe and respectful digital community.

Assessment:

a. An informal assessment can be made based on student participation in discussions and the activity.

Stewardship Scenarios:

1. **Friend Request from a Stranger:**

   Scenario: You receive a friend request from someone you don't know. They have no mutual friends with you, but their profile picture looks nice.

   Question: What should you do, and why?

2. **Tagging Without Permission:**

   Scenario: A friend tags you in an embarrassing photo and posts it on social media. You don't want others to see it, but they think it's funny.

   Question: How can you handle this situation respectfully?

3. **Password Sharing:**

   Scenario: Your friend gives you their social media password so you can help them with something. They ask you not to tell anyone.

   Question: Is it okay to have your friend's password? What are some possible risks?

4. **Hurtful Comment:**

   Scenario: You see a hurtful comment on one of your friend's posts. They haven't noticed it yet, and the person who posted it is someone you know.

   Question: What would a responsible digital steward do in this situation?

5. **Inappropriate Content:**

   Scenario: A friend sends you a link to a website that has inappropriate or offensive content. They say, "It's just for fun."

   Question: How should you respond, and what could you do next?

6. **Group Chat Drama:**

   Scenario: In a group chat, someone starts spreading a rumor about another person in your class. Some people join in, while others stay silent.

   Question: What could you do to practice good stewardship in this situation?

7. **Sharing Without Consent:**

   Scenario: You're at a party, and you take a funny video of a friend. You think it would be fun to post it online, but they haven't seen the video yet.

   Question: What's the best way to handle this, and why?

8. **Suspicious Link:**

   Scenario: You receive a direct message from someone with a link and the message, “Check this out, it’s so cool!” You don’t recognize the sender, and the link looks unusual.

   Question: What should you do before clicking the link?

9. **Forwarding Messages:**

   Scenario: A friend sends you a personal message telling you about a tough time they’re going through. Later, you think about sharing it with another friend to get advice.

   Question: Should you share it, and what could you do instead to help your friend?

10. **Ignoring Terms and Conditions:**

    Scenario: You’re signing up for a new app, and it asks you to accept the terms and conditions. You’re in a rush, so you’re tempted to skip reading them and just agree.

    Question: What might a responsible digital steward consider in this situation?

TOC Title: G7 Environmental Stewardship
Lesson Title: Environmental Stewardship
Grade Level: 7
Duration: 45 minutes

Objectives:

- The students will understand environmental stewardship.
- The students will know what action to take in their communities.

Suggested Materials:

- Whiteboard/chalkboard.
- Paper or index cards.
- Markers or colored pencils.
- Optional: video related to the topic. Suggestion: *WHAT DOES ENVIRONMENTAL STEWARDSHIP MEAN,* https://www.youtube.com/watch?v=7RNAUxqpQ5w&t=207s (7 minutes 19 seconds), or a similar age-appropriate video.

Procedure

Introduction (10 minutes):

a. Define environmental stewardship as the responsible use and protection of the environment through sustainable practices.
b. Discuss why stewardship is essential (preserving natural resources, protecting biodiversity, ensuring a healthy planet for future generations).
c. Ask students what actions they think help or harm the environment.
d. Briefly brainstorm on the board about everyday actions that impact the environment positively or negatively.

Video (10 minutes):

a. Optional: Show video related to topic. Suggestion: *WHAT DOES ENVIRONMENTAL STEWARDSHIP MEAN*, https://www.youtube.com/watch?v=7RNAUxqpQ5w&t=207s, or a similar age-appropriate video.
b. Briefly discuss with students what they learned from the video.

Activity (20 minutes)

a. Brainstorming (5 minutes): Ask students to think of actions that reduce waste, save energy, or protect nature. Write some examples on the board (e.g., using reusable water bottles, turning off lights, recycling).

b. Eco-Challenge Cards (10 minutes): Students create “Eco-Challenge” cards with an action they pledge to take to help the environment. Students write their actions on one side and decorate the other with drawings related to their pledge.
c. Sharing and Goal Setting (5 minutes): Ask for volunteers to share their eco-challenge with the class. Students can then take their cards home as a reminder or place them on a class bulletin board as a collective goal to promote stewardship.

Conclusion (5 minutes):

a. Reflection Questions Ask:
    - Why is it important to take care of the environment?
    - How does our class’s effort make a difference?
b. Encourage students to reflect on the changes they could make and inspire family members or friends to participate.

Assessment:

a. An informal assessment can be taken based on student participation in discussions and activity.

Grade 8

TOC Title: G8 Stewardship

Lesson Title: Stewardship
Grade Level: 8
Duration: 45 minutes

Lesson Objectives:

- The students will understand digital stewardship and responsible technology use.
- The students will be able to Identify ways to protect personal information and respect others online.
- The students will understand the importance of being an ethical digital citizen.

Suggested Materials:

- Whiteboard and markers.
- Digital Stewardship Challenge handouts (provided below).
- Pencils and paper for activity and conclusion.

Introduction (10 minutes):

a. Bring the group: Ask students if they have ever had a bad online experience or witnessed something inappropriate online. Let a few share briefly.
b. Introduce the idea of digital stewardship explaining that it involves being responsible and ethical with technology, treating it like a shared space where everyone feels safe and respected.
c. Discussion questions:
    i. What are some ways we can show responsibility when using digital tools?
    ii. How can we make sure we protect ourselves and respect others?

Mini-Lesson on Digital Stewardship: (10 minutes):

a. Discuss key aspects of digital stewardship such as protecting passwords, sharing content responsibly, and being aware of online dangers.
b. Offer examples of responsible and irresponsible behavior online.
    i. Responsible: Using privacy settings, asking permission before sharing photos.
    ii. Irresponsible: Sharing passwords with friends, spreading rumors online.
c. Encourage students to ask questions and share their thoughts.

Activity: Digital Stewardship Challenge (20 minutes):

a. Divide the class into small groups (three to four students per group).
b. Each group receives a Digital Stewardship Challenge scenario handout.

c. Each group works to decide what the most responsible action would be in each scenario and why.
d. Have groups share their answers with the class. After each group shares, ask other students if they agree or would handle it differently.

Conclusion (5 minutes):

a. Ask students to write down one action they will take to be a better digital steward.
b. Summarize key points and emphasize the importance of creating a safe digital environment for everyone.

Assessment:

a. An informal assessment can be taken based on student participation and contribution to group discussion and activity.

Scenario 1: Stranger Request:
You receive a friend request from someone you do not know. Their profile picture looks friendly, and they have mutual friends with you.

- **Question**: What should you do, and why?

Scenario 2: Password Sharing:
Your friend forgot their password to a shared game you both play and asks if you can give them yours so they can log in to your account.

- **Question**: Should you share your password? Why or why not?

Scenario 3: Embarrassing Post:
You come across an embarrassing photo of a classmate that someone posted online. Some of your friends are commenting and laughing at it.

- **Question**: What is the most responsible action you could take here?

Scenario 4: Group Chat Drama:
In a group chat, some friends start gossiping about a classmate and making fun of them. They encourage you to join in.

- **Question**: How would a digital steward respond to this?

Scenario 5: Clicking Suspicious Links
You get a message from a friend that has a link and says, “Check this out! You will not believe what you will see!” The link looks strange, and you are not sure if it is safe.

- **Question**: What should you do?

Scenario 6: Oversharing Online:
You are excited about your upcoming birthday party and want to post all the details online, including the time, location, and who is invited.

- **Question**: What is the best way to share this information without compromising safety?

Scenario 7: Consent in Photos:
You took a funny photo of a friend at school, and you want to post it on social media. Your friend is not sure if they want it shared.

- **Question**: What should you do before posting?

Scenario 8: Online Arguments:
You see a comment on one of your posts that you do not agree with, and it upsets you. You feel tempted to reply with an angry message.

- **Question**: How would a responsible digital steward handle this?

Scenario 9: Location Sharing:
A new app you downloaded asks for permission to access your location so it can "enhance your experience." You are not sure if you need this feature to use the app.

- **Question**: What should you consider before allowing location access? What would a digital steward do?

Scenario 10: Fake News and Rumors:
You see a shocking story about a celebrity or classmate online, and you are tempted to share it with your friends. It sounds interesting, but you are not sure if it is true.

- **Question**: How can you verify if the story is true? What is the responsible action here?

TOC Title: G8 Environmental Stewardship

Lesson Title: Environmental Stewardship
Grade Level: 8
Duration: 45 minutes

Objective:

- The students will understand the concept of environmental stewardship and its importance.
- The students will know and be able to use strategies to positively impact the environment.

Suggested Materials:

- Whiteboard/chalkboard.
- Markers or chalk.
- Printed handouts.
- Poster paper or large sheets of paper.
- Markers for the activity.
- Video related to the topic. Suggestion: *What is Sustainability*, https://www.youtube.com/watch?v=zx04Kl8y4dE (3 minutes 6 seconds), or a similar age-appropriate video

Procedure

Introduction (10 minutes):

a. Whole group: Ask students what they think environmental stewardship means.
b. Define environmental stewardship as taking care of and preserving natural resources.
c. Discuss real-world examples, such as recycling, conserving water, and protecting wildlife habitats.

Video and Discussion (10 minutes):

a. Show a short video related to the topic. Suggestion: *What is Sustainability*, https://www.youtube.com/watch?v=zx04Kl8y4dE, or a similar age-appropriate video.
b. Briefly discuss with students what they learned from the video.

Activity (20 minutes):

Activity: Stewardship Action Posters (20 minutes)

a. Divide the class into small groups (three to four per group) and assign each team a theme related to environmental stewardship (e.g., recycling, water conservation, reducing pollution).
b. Each team will create an environmental stewardship poster that highlights why their theme is essential and lists steps individuals can take to contribute.
c. Share and Discuss: Allow each group to present their poster briefly, encouraging open discussion and questions from classmates.

Conclusion (5 minutes):

a. Summarize key points about environmental stewardship.
b. Encourage students to commit to one actionable step they can take to be better environmental stewards.

Assessment:

a. An informal assessment can be taken based on student participation in discussions and activity.

Notes

1 Marcella, A., October 7, 2024, "Eight Types of Stewardship," Figure 4.1, designed and drawn by the author.

2 (n.a.), (n.d.), "Cultural Stewardship – Definition," https://library.fiveable.me/key-terms/native-people-their-environment/cultural-stewardship, retrieved September 30, 2024.

3 (n.a.), July 5, 2022, "Understanding Generation Alpha Characteristics – How They Are," https://www.studentcenteredworld.com/generation-alpha/, retrieved September 20, 2024.

4 (n.a.), (n.d.), "Responsibility for Your 12-Year-Old," https://parentingmontana.org/responsibility-for-your-12-year-old/, retrieved June 27, 2024.

5 Tucker, D., Andrews, B., & Hayes, K., "Student-Driven Stewardship Projects Using Environmental Education to Promote the Use of Science Practices," National Science and Teaching Association, Student-driven Stewardship Projects | NSTA, www.nsta.org/science-and-children/science-and-children-septemberoctober-2020/student-driven-stewardship-projects, retrieved December 15, 2023.

6 (n.a.), (n.d.), "Raising Children to be Good Stewards of the Earth," Raising Children to be Stewards of the Earth | Lesley University, https://lesley.edu/article/raising-children-to-be-stewards-of-the-earth, retrieved August 2, 2025.

7 Hurwitz, R., March 18, 2012, "Taking Care: Four Takes on the Cyber Steward," Proceedings of the CyberDialogue 2012: What is Stewardship in Cyberspace?, Canada Centre for Global Security Studies (Canada Centre) at the Munk School of Global Affairs at the University of Toronto, DSpace @MIT, https://dspace.mit.edu/handle/1721.1/141682#:~:text=Stewardship%20denotes%20a%20custodial%2C%20non,some%20technological%20advantage%20over%20others, retrieved October 7, 2024.

8 Tatter, G., October 7, 2018, "A Toolkit for Digital Civics," Harvard Graduate School of Education, www.gse.harvard.edu/ideas/usable-knowledge/18/10/toolkit-digital-civics?utm_medium=email&utm_source=govdelivery, retrieved October 7, 2024.

9 Oregon Department of Education, February 6, 2023, "Digital Learning Quarterly Newsletter from ODE," www.oregon.gov/ode/schools-and-districts/grants/Documents/Feb%202023%20Digital%20Learning%20Quarterly%20Newsletter%20from%20ODE.pdf, retrieved October 11, 2024.

10 Oregon Department of Education, July 2021, "Key Components of Digital Learning: A Starting Point for Design, Dialogue, and Implementation Version 1.0," Figure 4.2, redrawn by author, www.oregon.gov/ode/educator-resources/teachingcontent/EdTech/Documents/ODE_Digital%20Learning%20Playbook.pdf?utm_medium=email&utm_source=govdelivery, retrieved October 11, 2024.

11 Oregon Department of Education, July 2021, "Key Components of Digital Learning: A Starting Point for Design, Dialogue, and Implementation Version 1.0," www.oregon.gov/ode/educator-resources/teachingcontent/EdTech/Documents/ODE_Digital%20Learning%20Playbook.pdf?utm_medium=email&utm_source=govdelivery, retrieved October 11, 2024.

12 Pratt, J., August 11, 2022, "What Is Digital Citizenship? Be Empowered to Teach These Essential Skills," gabb, https://gabb.com/blog/what-is-digital-citizenship/, retrieved October 14, 2024.

13 Hobbs, R., Chapman, D., Doerr-Stevens, C., et al., April 9, 2022, "Media Education in English Language Arts," National Council of Teachers of English, https://ncte.org/statement/media_education, retrieved October 7, 2024.

14 Jones, L.M., & Mitchell, K.J., 2016, "Defining and Measuring Youth Digital Citizenship," *New Media & Society*, 18(9), 2063–2079. https://doi.org/10.1177/1461444815577797, retrieved October 10, 2024.

15 Marcella, A., October 10, 2024, "Choi's Four Categories of Digital Citizenship," Figure 4.3, designed and drawn by the author.

16 Choi, M., 2016, "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age," *Theory & Research in Social Education*, 44(4), 565–607, http://global-awareness.org/resources/misc/Choi2016ConceptAnalysisDigitalCitizenship.pdf, retrieved October 11, 2024.

17 Ribble, M., July 26, 2021, "Essential Elements of Digital Citizenship," The International Society for Technology in Education (ISTE), https://iste.org/blog/Essential-elements-of-digital-citizenship, retrieved on October 11, 2024.

18 Stone, R., February 16, 2024, "Collaboration: A Key to Effective Leadership," *Psychology Today*, www.psychologytoday.com/us/blog/the-color-of-wellness/202402/collaboration-a-key-to-effective-leadership, retrieved October 23, 2024.

19 Burress, D., May 15, 2020, "The Importance of Stewardship in Leadership," Graduate Programs for Educators, The Importance of Stewardship in Leadership – Graduate Programs for Educators, retrieved December 15, 2023.

20 VOLUNTEER | English meaning – Cambridge Dictionary.

21 (n.a.), (n.d.), "Befits of Volunteering." Western Connecticut State University, https://www.wcsu.edu/community-engagement/benefits-of-volunteering/#:~:text=Volunteering%20allows%20you%20to%20connect,animals%2C%20and%20organizations%20in%20need., retrieved September 30, 2024.

22 Shutterstock, October 30, 2024, Figure 4.4 "Plant Earth - Environmental Sustainability," Stock Vector ID: 348618227, used under CRC License.

23 (n.a.), (n.d.), https://www.earthday.org/, retrieved June 27, 2024.

24 (n.a.), (n.d.), "Earth Day 2023: 5 Earth Day Facts to Know about and How to Get Involved | Earth.Org," retrieved June 27, 2024.

25 (n.a.), (n.d.), "Teaching about Earth Day," Educators4SC, Teaching about Earth Day – Educators 4SC, retrieved June 27, 2024.

26 Cordone, E. C., Centeno, D., & Todd, A. M., 2020, "The Role of Climate Change Education on Individual Lifetime Carbon Emissions," *PLoS One*, 15(2), e0206266, https://doi.org/10.1371/journal.pone.0206266, https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0206266, retrieved March 1, 2024.

27 Rideout, V., Peebles, A., Mann, S., & Robb, M. B., 2022, Common Sense Media, "The Common Sense Census: Media used by Tweens and Teens, 2021," Page 15, www.commonsensemedia.org/sites/default/files/research/report/8-18-census-integrated-report-final-web_0.pdf, retrieved September 22, 2024.

28 Lewis, J., March 2021, "Stewardship, Security, and Cyberspace," Center for Strategic and International Studies Washington, DC; Cyberdialogue2012: What is Stewardship in Cyberspace?, https://cyberdialogue.ca/wp-content/uploads/2012/2012papers/CyberDialogue2012_Lewis.pdf, retrieved October 26, 2024.

29 The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents the right to have access to their children's education records, the right to seek to have the records amended, and the right to have some control over the disclosure of personally identifiable information from the education records. When a student turns 18 years old or enters a postsecondary institution at any age, the rights under FERPA transfer from the parents to the student ("eligible student"). The FERPA statute is found at 20 U.S.C. § 1232g and the FERPA regulations are found at 34 CFR Part 99.

30 Parisi, M., 2024, "Sustainability Word Find Puzzle," Figure 4.5, created by authors.

31 Parisi, M., 2024, "Sustainability Word Find Puzzle - Solution," Figure 4.6, created by authors

Epilogue

As a mental health therapist for adolescents, I've seen how technology affects young people's mental health. Smartphones, social media, and online gaming can worsen issues like depression, anxiety, and social isolation. These impacts often start subtly, showing up as changes in behavior, emotional distress, and difficulties in relationships.

From Street-smart to Web-wise® is written for you, educators, teachers, and all those who spend a lot of time with students and are often the first to notice these signs. In the classroom, shifts in mood and focus become clear, allowing educators to address these concerns effectively. It's essential for both students and educators to understand Internet safety and also the emotional effects of online behavior. Along with the authors, I hope this manual makes you better prepared to identify, respond, and assist your students.

From Street-smart to Web-wise® addresses the link between technology, education, and mental health, and that you feel better equipped with the knowledge and tools to promote safer online habits among students and to address the mental health implications of technology use.

The comprehensive guide offered in *From Street-smart to Web-wise*® was designed to empower teachers and help connect Internet safety skills with a supportive learning environment.

I commend the authors for their vision and dedication to this important work! Together we can promote a future where technology empowers young people and supports their mental health.

— **Sara Malcom,** *Mental Health Therapist, Gilbert, Arizona*

Appendix A: Teacher's Resource List

The following materials represent a non-exhaustive list of supplemental teaching resources that the educator may find both of interest and use in developing class instructional materials to further the cyber-safe education of young learners. The resources are presented alphabetically, and the URL included with each resource is the most current as of November 2024.

Blogs

Sleepovers in the Digital Age, Haley Zapal, February 25, 2019, The Bark Blog. A deep dive into the pros and cons of taking phones away at sleepovers and provide a path that may satisfy both camps.

Classpoint.com

Understanding Gen Alpha slang will help understand what your students are saying and help you connect with them.

50 Gen Alpha Slangs You Need To Speak Their Language In Class | ClassPoint

CBS News Video Resources — Online Scams

In Finland, Teaching Students To Spot Disinformation And Fake News (Video).

Being able to identify hoaxes, avoid scams, and debunk propaganda is a civic skill required in today's information society. That's why the curriculum of students in Finland includes media literacy lessons, aimed at safeguarding a precious resource: the truth.

Chris Livesay, www.cbsnews.com/news/this-week-on-sunday-morning-september-29-2024/

How CBS News Tracked Down Ghanaian Romance Scammers Duping Americans Into Parting With Huge Sums Of Money (Video).

Debora Patta, Sarah Carter, Meshack Dube, September 27, 2024, www.cbsnews.com/news/ghana-romance-scammers-duping-americans/

Children's Illustrated Books

"Bullies Never Win" by Margery Cuyler and Arthur Howard — Standing up for oneself is the theme of this book [ISBN 13: 978-0689861871].

"Hello Ruby: Journey Inside the Computer" by Linda Liukas — A fun and interactive way to learn about computers and technology for kids [ISBN 13: 978-1250065322].

"Kidpower Children's Safety Comics Color Edition: Use *Your Power to Stay Safe*!" Have fun while teaching kids to be safe from bullying, abuse, and violence. The books have updated social stories and skills, including how to help kids stay safe online. The tools in this comic book are most appropriate for parents, teachers, and other caregivers introducing "People Safety" to children who are usually with adults who can help them [www.kidpower.org/books/kidpower-childrens-safety-comics-color-edition].

"Kindness is Cooler, Mrs. Ruler" by Margery Cuyler and Sachiko Yoshikawa is another illustrated book that is great for starting conversations about kindness, a key element of character education [ISBN 13: 978-0689873447].

"Stand in My Shoes: Kids Learning about Empathy" by Bob Sornson — This book, while not a comic, uses engaging illustrations and storytelling to teach kids about empathy [ISBN 13: 978-0578807942].

Crisis and Intervention

Crisis TEXT Line. Bullying Resources | Text HOME to 741741 for free support (crisistextline.org)

Need help? Text HOME to 741741. Need to talk? Call 1-800-273-TALK (8255) anytime if you are in the United States. It's free and confidential.

Stomp Out Bullying: Bullying Help | STOMP Out Bullying™ HelpChat Crisis Line

The STOMP Out Bullying™ HelpChat Crisis Line is a free and confidential **online chat** that helps youth ages 13–24 (not a place for adults over 24) with issues around bullying and cyberbullying, as well as providing support to youths who may be at risk of suicide.

Cyber Safety Research

Finkelhor, D., Walsh, K., Jones, L., Mitchell, K., & Collier, A., 2021, "Youth Internet Safety Education: Aligning Programs with the Evidence Base," *Trauma, Violence, & Abuse*, 22(5), 1233–1247. https://doi.org/10.1177/1524838020916257.

[This research reviews the literature on online harms to children and discusses how to develop effective online safety messages.]

Ofcom.org, (n.a.), "Children and Parents: Media Use and Attitudes Report 2022," (ofcom.org.uk). [This report looks at media use, attitudes, and understanding among children and young people aged 3–17.]

Ondrušková, D., & Pospíšil, R., 2023, "The Good Practices for Implementation of Cyber Security Education for School Children," *Contemporary Educational Technology*, 15(3), Article No. ep435, ISSN: 1309-517X (Online), https://doi.org/10.30935/cedtech/13253. [Outlines best practices for implementing cybersecurity education in schools, emphasizing age-appropriate methods.]

Wishart, J., 2004, "Internet Safety in Emerging Educational Contexts," *Computers & Education*, 43, 193–204. https://doi.org/10.1016/j.compedu.2003.12.013, www.researchgate.net/publication/220140831_Internet_safety_in_emerging_educational_contexts/citation/download. [This paper reports on the consequent audit of Internet Safety practices in over 500 schools from 27 Local Education Authorities across England, commissioned by Becta and conducted during the summer term 2002.]

Moynihan, M., November 28, 2014, "Using Web 2.0 tools to teach online safety education in the intermediate grades," Vancouver Island University, https://viuspace.viu.ca/bitstream/handle/10613/2328/MoynihanOLTD.pdf?sequence=3. [Demonstrates how Web 2.0 tools can be effectively used in teaching online safety to young students.]

Hartikainen, H., Iivari, N., & Kinnula, M., December 2019, "Children's Design Recommendations for Online Safety Education," *International Journal of Child-Computer Interaction*, 22, 100146, ISSN 2212-8689, https://doi.org/10.1016/j.ijcci.2019.100146, www.sciencedirect.com/science/article/pii/S2212868917300764. [Focuses on involving children in the design of online safety education, ensuring that the content is relatable and understandable for them.]

Digital Resources

BrainPOP Jr. Internet Safety Video — A resource for teaching children about interacting with strangers online and protecting private information. Includes activities such as Word Play and Write About It, along with quizzes for assessment [https://jr.brainpop.com/artsandtechnology/technology/internetsafety].

Georgia Public Broadcasting (GPB) — GPB Education is Georgia's digital media content provider for the classroom offering locally produced, Georgia-specific content and digital streaming services across all subject areas to teachers and students. GPB's goal is to remain at the forefront of the digital learning movement by creating, curating, and distributing quality educational programs and services through a state-of-the-art production facility, cutting-edge digital media division, and a partnership with PBS LearningMedia.

GPB Education also provides training for Georgia's educators and educational institutions [www.gpb.org/education/learn/school-stories/science-in-action]

Mentoring Youth — Provides resources and tools for mentoring youth (https://nationalmentoringresourcecenter.org/resources-for-mentoring-programs/)

National Alliance on Mental Illness (NAMI) — In addition to NAMI's support of mental illness, they provide resources for bullying, a teen and youth call center, stress management, and much more [www.nami.org/Home].

National Alliance on Mental Illness (NAMI) — Back to School Resources: This resource is specifically designed to support educators, guide parents, and empower students on their mental health journey during the school year and beyond (Back to School Resources | NAMI).

Neuroscience in Education — Center for Educational Neuroscience: A component of Mind Brain and Education is an emerging scientific field that brings together researchers in cognitive neuroscience, developmental cognitive neuroscience, educational psychology, educational technology, education theory, and other related disciplines to explore the interactions between biological processes and education [www.educationalneuroscience.org.uk/about-us/what-is-educational-neuroscience].

Generative Artificial Intelligence (AI) Tools

Writing Assistants

- AI-Writer: An AI writing assistant that helps reword and remediate an existing piece of content, creates unique article drafts, provides citation lists, summarizes search engine optimization (SEO) competitors (a competitor, in the context of SEO, is a website or web page that is competing with your target page for ranking in the search engine results), and creates SEO-optimized content from Google. SEO is the process of improving the quality and quantity of website traffic to a website or a web page from search engines
- Bard: Google's conversational AI tool. Bard aims to improve the way people search for and retrieve information.
- ChatSonic: A dialogue-focused content generator from Writesonic built on top of GPT-4 with added features. Users can choose from 16 different personas to chat with, including poets and accountants.
- Claude: A conversational AI tool by Anthropic, which is integrated into Slack to summarize threads and answer questions.
- Docs: Google's cloud-based, collaborative word processor with AI features to generate, summarize, and brainstorm text.
- Freshchat: A chatbot platform that can be used in education. It can engage in dialogue with students, identify gaps in learning, provide relevant information, answer questions, and suggest alternative strategies. Freshchat can act

as a virtual teaching assistant, reducing the teacher's workload and helping students get back on track.

- Grammarly: The mainstream spell and structure-checking app. It assists users in keeping their grammar on point, lets writers adjust their tone, and suggests shortcuts to simplify wordy or complex phrases.
- Jasper AI: A long-form AI copywriting tool and article generator that includes more than 50 content generation templates in 25 global languages.
- Koala: An AI chatbot that can assist students and teachers with generating long-form written pieces such as essays and blog posts. It offers references and sources for its data and is built on advanced AI technology. Koala can understand variations in user input and pick up on conversational contexts, making it a helpful tool for writing assignments.
- Magic Write: An AI text generator for Canva Docs. Users can prompt Magic Write to brainstorm, generate outlines, and generate content ideas.
- Perplexity AI: An AI-powered search engine. A unique feature of Perplexity is that it can provide sources to back up the answers that it has generated. It functions more as a search engine than an original writer but still generates original content.
- Rytr: An AI content generator that lets content creators specify a content use case, tone of voice, and keywords.
- Spellbook: A writing software by Rally that is designed to help lawyers with legal drafting. Spellbook can draft new contract clauses, list common negotiation points based on the contract, and create contract summaries.
- Tome: Utilizes advanced language models to generate text based on user input or prompts. Tome can be used for various purposes such as brainstorming ideas, generating story outlines, or even crafting entire passages of text.
- Wordtune: Assists users in improving their writing by providing suggestions and alternatives for phrases and sentences by offering suggestions for rewriting sentences to enhance clarity, coherence, and style, helping users refine their writing quickly and effectively.

Image Design and Development

- Craiyon: Produces a batch of AI-generated images in response to a text prompt.
- DALL-E: An OpenAI's image generator that creates images and art from a simple text prompt.
- Image Creator: Designed to produce images based on user inputs or predefined parameters in the creation of graphic design, art creation, or even generating visual content for websites and presentations.
- ImageFX: A Google's innovative AI-powered image generation tool, enabling users to create images from simple text prompts.

- Stable Diffusion: A Stability AI's generator that can create photorealistic images from an inputted text.

Music

- Amper Music: A generator that creates music from prerecorded samples. The software can be used to match music to video.
- Dadabots: A generative neural network that creates a constant live stream of artificial music in different genres and raw audio neural networks that imitate bands.
- Soundraw: An AI music generator that can be used to generate royalty-free background music.

Others

- Bing: While not a generative AI tool, it is a search engine developed by Microsoft. Bing provides users with the ability to search for information, images, videos, and news on the Internet. It utilizes algorithms to index web pages and deliver relevant search results based on user queries.
- Character AI: Focuses on creating lifelike characters for various digital applications by generating dialogues, personalities, and backstories for virtual characters in games, simulations, or interactive storytelling platforms. Character AI provides developers and storytellers with a powerful tool for crafting compelling narrative experiences in digital environments.
- Creo: A computer-aided design system that uses generative design, enabling expedited design of physical objects. It also optimizes designs based on material and manufacturing requirements.
- Grok: An xAI's — Elon Musk's AI startup — version of ChatGPT. It has Internet browsing capability and can answer users based on up-to-date information on the web.
- Jasper Chat: Focuses on creating conversational experiences designed to engage users in natural and fluid conversations, simulating human-like interactions. It can be utilized in various applications such as interactive storytelling platforms.
- OpenAI GPT-3 Playground: Allows users to interact with and explore the capabilities of the GPT-3 language model. Users can input text prompts and receive generated responses from GPT-3 in real-time, enabling experimentation with various language tasks such as writing, summarization, translation, and more. The playground provides a user-friendly interface for developers, researchers, and enthusiasts to understand, test, and leverage the power of GPT-3 for a wide range of applications.
- Pi: A chatbot designed to serve as the user's personal assistant.[1]
- PepperType: It is specifically tailored for text generation tasks including content creation, creative writing, and text summarization.

- Perplexity.ai: Has access to the Internet and current events and provides prompt suggestions to get chats started.
- Replika: This app is designed to simulate conversational interactions with users effectively mimicking human conversation. It serves as a virtual companion, aiming to foster meaningful connections and support mental well-being through its conversational interface.
- Socratic: Children can type in any question they may have about what they are learning in school, and Socratic will generate a conversational, human-like response with fun unique graphics to help break down the concept.
- YouChat: Outputs an answer to anything you input including math, coding, translating, and writing prompts. This chatbot cites sources from Google, which ChatGPT does not because ChatGPT doesn't have Internet access.

Instructional Resources

Common Sense Education — 23 Great Lesson Plans for Internet Safety — Provides lesson plans to help students build critical-thinking skills and navigate online dilemmas [www.commonsense.org/education/articles/23-great-lesson-plans-for-internet-safety].

Common Sense Education Safety in My Online Neighborhood — Offers lesson plans for digital citizenship that address timely topics such as cyberbullying, cybersecurity, identity verification, physical security, and online safety. Their curriculum is research-backed and designed to help schools navigate these issues with their students. Lesson plans culminate in interactive activities like the Internet Traffic Light game, where students assess whether the presented online content is appropriate or not [www.commonsense.org].

Edutopia — Provides a lesson plan for teaching Internet safety to students as young as kindergarten. The plan includes discussions about strangers online and protecting private information. Additional activities such as watching an Internet safety video, quizzes, and creating safety posters are also outlined [www.edutopia.org].

EVERFI — The Compassion Project — A free empathy curriculum for second to fifth graders, designed to facilitate lessons around social and emotional skills [https://everfi.com/k-12/character-education].

GoodCharacter.com — Character Education & Social Emotional (SEL) Learning Resources — Provides teaching guides for K—12 on character education and social-emotional learning, covering topics like mindfulness, conflict resolution, and bullying.

  - Bullying [www.livewiremedia.com/product-category/bullying]
  - Citizenship Guides [www.livewiremedia.com/product-category/citizenship]
  - Conflict Resolution [www.livewiremedia.com/product-category/conflict-resolution-2]

- Fairness [www.livewiremedia.com/product-category/fairness]
- Good Character Teaching Guides [www.livewiremedia.com/product-category/character-education] and [www.livewiremedia.com/product-category/character-counts]
- Manners and Politeness [www.livewiremedia.com/product-category/manners-politeness]
- Mindfulness [www.livewiremedia.com/product-category/mindfulness]
- Respect [www.livewiremedia.com/product-category/respect]
- Social Media & Internet Safety [www.livewiremedia.com/product-category/social-media-internet-safety-2]

Middle Grades Research Journal (MGRJ) — A refereed, peer-reviewed journal that publishes original studies providing both empirical and theoretical frameworks that focus on middle grades education. IAP – Information Age Publishing, Inc., PO Box 79049, Charlotte, NC 28271-7047, 704.752.9125, email: infoage@infoagepub.com, www.infoagepub.com.

Safer, Smarter Kids Curriculum — A comprehensive program that covers various safety topics, including cyber safety, body boundaries, and recognizing unsafe situations [https://safersmarterkids.org].

Scratch (https://scratch.mit.edu) — A visual programming language used to create simple chatbot-like programs.

TeacherVision Safety Printables and Activities — Offers a wide array of lesson plans, printables, and resources, including content for teaching Internet safety [www.teachervision.com/subjects/health-safety/safety].

United Nations Office on Drugs and Crime (UNODC) Primary Lesson Plan for Staying Safe Online — While this resource is more general, it does include exercises and additional teaching tools that can be adapted for younger students [www.unodc.org/e4j/en/primary/e4j-tools-and-materials/lesson-plan_staying-safe-online.html].

Interactive Assessment Exercises

Cyber Awareness & Safety Education (CASE) — This curriculum offers a series of interactive classes where students actively learn through videos, case studies, and group discussions. The end-of-course test measures mastery of the material. This program includes pretests and posttests to assess student understanding of Internet safety, along with active learning techniques to personalize the topics covered [www.cybersafetyconsulting.com].

Interactive Games and Classroom Exercises

CISA Cybersecurity Awareness Program Student Resources — Offers downloadable activity sheets, books, and other resources for young children on cyber safety. It also includes games from the FBI's Safe Online Surfing program and tips from the National Cyber Security Alliance.

- Savvy Cyber Kids [https://savvycyberkids.org]
- Safe Online Surfing by FBI [https://sos.fbi.gov/en]
- NetSmartz Kids [www.netsmartzkids.org]

Digital Well-being Packet and Classroom Activities from Be Internet Awesome — A multifaceted program that includes both a game called Interland to engage students in learning about online safety and a curriculum for educators to teach kids how to be safe and responsible online. They also offer a pledge for families to promote online safety at home.

The site provides comprehensive guides and printable activities to support educators in introducing digital well-being to students. Lesson plans for five topics with activities and worksheets designed to complement the Interland game, focusing on being smart, alert, strong, kind, and brave online. It also provides interactive, game-based activities that assess students' understanding of Internet safety in a fun and engaging way [https://beinternetawesome.withgoogle.com/en_us/educators].

Safety Land by AT&T — An interactive game for elementary students that teaches Internet safety in a fun and engaging way [https://freetech4teach.teachermade.com/2011/04/at-safety-land-cyber-safety-game-for].

NPR Video Resources

Lizarraga, L., November 8, 2023, How does a computer discriminate? www.npr.org/2023/11/08/1197954253/how-ai-and-race-interact.

Mosley, T., November 28, 2023, "'If you have a face, you have a place in the conversation about AI,' expert says," www.npr.org/2023/11/28/1215529902/unmasking-ai-facial-recognition-technology-joy-buolamwini.

Podcasts

MIT's Anant Agarwal on AI in Education — Ep. 197
The AI Podcast
June 7, 2023
https://soundcloud.com/theaipodcast/edtech?utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing

Education and AI: What Does AI Have to Teach Us?
Technically Optimistic
July 21, 2023
https://podcasts.apple.com/us/podcast/education-and-ai-what-does-ai-have-to-teach-us/id1689164209?i=1000621942866

The TED AI Show

Creative technologist Bilawal Sidhu talks with the world's leading experts, artists, journalists, and more to explore the thrilling, sometimes terrifying, future ahead.

https://podcasts.apple.com/us/podcast/the-ted-ai-show/id1741574582

Publications

15-Minute Focus: Digital Citizenship: Supporting Youth Navigating Technology in a Rapidly Changing World
Raychelle Cassada Lohmann and Angie C. Smith
National Center for Youth Issues
May 4, 2023
ISBN-13: 978-1953945778

An Educator's Guide to AI in the Classroom: The Transformative Power of AI in Education, How to Use AI in School, K — 12 Classroom Lesson Plans, and Answers to Common AI Questions
Abigail McKeag
ViaNova Productions, LLC
July 24, 2023
ISBN-13: 979-8988586296

Developing Digital Detectives: Essential Lessons for Discerning Fact from Fiction in the "Fake News" Era
Jennifer LaGarde, Darren Hudgins
International Society for Technology in Education
September 27, 2021
ISBN-13: 978-1564849052

Digital Citizenship Handbook for School Leaders: Fostering Positive Interactions Online
Mike Ribble and Marty Park,
International Society for Technology in Education
June 26, 2019
ISBN-13: 978-1564847829

Ethics in a Digital World: Guiding Students Through Society's Biggest Questions
Kristen Mattson
International Society for Technology in Education
April 19, 2021
ISBN-13: 978-1564849014

LGBT Teens, Bullying, and Suicide — Child Mind Institute — The Child Mind Institute serves children and families struggling with mental health and learning disorders.

TED-Ed Video Resources

Note: TED-Ed is TED Talk's [www.ted.com/talks] youth and education initiative.

For Teachers:
Shane Koyczan: To This Day ... for the bullied and beautiful | TED Talk
Sally Kohn: Don't like clickbait? Don't click | TED Talk
For Students:
Unintentional Bullying | TED Talk

"3 Questions to Ask Yourself about Everything You Do" – by Stacey Abrams: "How you respond to setbacks is what defines your character," a talk that could be adapted to discuss character and self-reflection, important components of character education [https://ed.ted.com/search?qs=%223+questions+to+ask+yourself+about+everything+you+do%22+].

"Grit: The Power of Passion and Perseverance" – by Angela Lee Duckworth: This talk may be adapted to be used to discuss the character trait of perseverance [https://ed.ted.com/search?qs=Grit%3A+The+Power+of+passion+and+perseverance].

"How to Build Your Confidence — and Spark It in Others" – by Brittany Packnett: This talk can help in discussions with students about self-confidence as a part of one's character [https://www.youtube.com/watch?v=b5ZESpOAolU&t=4s].

YouTube/Netflix Video Resources

"Being Respectful Video for Kids" | Character Education – by Jessica Diaz: This video can help teach kids about being respectful, an essential aspect of character education [https://www.youtube.com/watch?v=KxnxObAyfSA].

"Consequences for Kids" | Character Education – by Jessica Diaz: This video is designed to help children understand what consequences are and why they matter, reinforcing the concept of accountability [www.youtube.com/watch?v=LLZZYf_mlOA].

"Cyber Security for Kids" – by Neel Nation: This video is about being safe on the Internet. The video provides five tips for kids to be safe on the Internet. Being cyber-safe is very important as the kids are always online these days. This video talks about the importance of passwords, protecting personal information, limiting screen time, etc. [www.youtube.com/watch?v=nVEyG3C-Mqw].

"Cyberbullying – How to Avoid Cyber Abuse" – by Smile and Learn: This video showcases a series of situations related to how students can stop cyberbullying. Also discussed is the concept of being a good friend, not a bystander, and respecting privacy, and that actions can make a difference [www.youtube.com/watch?v=dMdKmHjpgFk].

"Cybersecurity Training for Kids" – by Malware Bytes: A fun video just for the kids, where they can learn all about Dr. Evil and her Internet schemes [www.youtube.com/watch?v=XiU72Vzs5Is].

"Internet Safety for Kids K — 3" by – Indiana University of Pennsylvania: This video is aimed at younger children and provides guidance on staying safe on the Internet [www.youtube.com/watch?v=89eCHtFs0XM].

"Internet Safety Tips for Kids" by – MoneyMoments (MidFirst Bank): This short video covers safety tips for your kids using the Internet [www.youtube.com/watch?v=qtJNRxMRuPE].

"Online Privacy for Kids – Internet Safety and Security for Kids"–by Smile and Learn: This video discusses the importance of online privacy and safety for children, which is crucial for their well-being in the digital age [www.youtube.com/watch?v=yiKeLOKc1tw].

"Online safety Staying Safe Online" – by Born in the USA: This resource features in Discovery Education Espresso's Online safety module. Learn how to stay safe and act responsibly when using the Internet in school and at home [www.youtube.com/watch?v=PtfEnh0gbbU].

"Private and Personal Information" – by Common Sense Education: It is natural for students to enjoy sharing and connecting with others. However, sharing information online can sometimes come with risks. This video addresses these risks [www.youtube.com/watch?v=MjPpG2e71Ec].

Web of Make Believe — This Netflix series comes with a content warning. It is an anthology of true crime stories that shows the results of online misinformation. Web of Make Believe: Death, Lies and the Internet (TV Series 2022) - IMDb. Common Sense Media recommends this for ages 15+. It is a good resource for teachers and others to understand the misuse online and how it impacts children. Web of Make Believe: Death, Lies, and the Internet TV Review | Common Sense Media

know2protect.gov — US Department of Homeland Security (DHS) Series: This series provides short videos to help understand the importance of online vigilance and information to retain in various situations.

Digital Safety Series: Know the Threats

Digital Safety Series: What To Do If Something Happens

Web Sites

Code.org

Offers beginner coding activities that help understand the basics of programming, including chatbots.

Common Sense Education (www.commonsense.org/education/digital-citizenship/internet-safety)

Expert-tested resources for K — 12 educators including scope and sequence, lesson plans, and a digital citizenship program. Also includes resources for parents and a step-by-step community involvement guide.

Cyberpatriot (www.uscyberpatriot.org/competition/training-materials/training-modules)

Air Force Association archived online training modules cover topics such as cyber ethics, cybersecurity, and online safety.

Cyberpatriot Elementary School Cyber Education Initiative (www.uscyberpatriot.org/Pages/Special%20Initiatives/Elementary-School-Initiative.aspx)

Three interactive learning modules created to increase K — 6 students' online safety awareness.

Cyberwise (www.cyberwise.org/digital-citizenship-resources)

This site combines in-depth research with a fully developed curricular unit (cyber civics) to provide a wealth of resources for educators and parents. Higher education professionals might use research resources from this site in teacher education seminars.

Department of Justice (StopBullying.gov).

Although no federal law directly addresses bullying, in some cases, bullying overlaps with discriminatory harassment when it is based on race, national origin, color, sex (including sexual orientation and gender identity), age, disability, or religion.

Digital Parenting Pro | Parental Controls Guide | Vodafone UK

Vodafone is a UK-based multinational telecommunications company. The interactive Digital Parenting Pro resource provides helpful information about parental controls and safety settings available across the most popular apps, games, and devices.

Digizen (https://www.childnet.com/resources/looking-for-digizen/)

This interactive site is a comprehensive resource on digital citizenship for educators, parents, and students specifically targeting social media/networking sites and online etiquette.

Expert Parenting Tips and Online Safety - Kids n Clicks

Created by a teacher to help parents and teachers support their children, aiming to harness technology for its benefits and safeguard families from potential harm. Includes checklist to help guide guardians and parents.

Home - Leave No Trace - Leave No Trace (lnt.org)

Leave No Trace is a nonprofit using the power of science, education and stewardship, and is on a mission to ensure a sustainable future for the outdoors and the planet.

LEGO - Build and Talk - Sustainability (LEGO.com)

Covering six different topics, the activities are designed to help children navigate the online world safely. You'll also find handy discussion starters to get the conversation going as you Build & Talk together.

MBA Research — Course Package: Ethical Leadership for Middle-Level Students #BB-CG12-30
www.mbashop.org

Middle School Ethics Bowl — Ethics Institute
www.ethicsatkentplace.org

Middle School Ethics Education — MBA Research
www.mbaresearch.org/ethics/middle-school-ethics-education

Missing and Exploited Children
Provides information and a resource to help get inappropriate images taken down. Is Your Explicit Content Out There? (missingkids.org)

Office of Juvenile Justice and Delinquency Prevention (OJJDP) School-Based Bullying Prevention I-Guide (ojp.gov).
This Model Program I-Guide is focused on the problem of bullying in school and is intended for those interested in creating safe school environments by implementing school-based bullying prevention programs.

Plugged In
Plugged In is a Focus on the Family publication designed to shine a light on the world of popular entertainment while giving families the essential tools they need to understand, navigate, and impact the culture in which they live.

ScreenStrong: What Is ScreenStrong? | ScreenStrong | ScreenStrong
ScreenStrong empowers families to prevent screen addiction and reclaim their kids from problematic screen use (social media, video games, and pornography). Solutions are not screen-free, but to replace toxic screen use with healthy activities, life skill development, and family connections.

Smart Social [SmartSocial.com]
Digital Citizenship programs. Resources to help parents & educators keep students safe on social media. Membership required.

he Ethics Institute — Kent Place School
ethicsatkentplace.org

Trigger Warning Database
Trigger warnings allow readers to be aware of a book's content beforehand, so they can make informed choices about what they choose to read and when they choose to read it.

Who We Are | Global Citizen
Global Citizens are action-takers and impact-makers. Our mission is to end extreme poverty worldwide now. Our voices inspire action to defend the planet, defeat poverty, and demand equity. We post, tweet, message, vote, sign, and call to influence leaders and citizens to act.

Note

1 Lutkevich, B., January 31, 2024, "34 AI Content Generators to Explore in 2024," TechTarget, https://www.techtarget.com/whatis/feature/AI-content-generators-to-explore?utm_campaign=20240206_ERU-ACTIVE_WITHIN_90_DAYS&utm_medium=email&utm_source=SGERU&source_ad_id=365530155&src=15006417&asrc=EM_SGERU_287913277, retrieved February 11, 2024.

Appendix B: Recommended Readings

The following titles represent a non-exhaustive list of recommended readings that the educator may find both of interest and use in furthering the cyber-safe education of their students. These reading resources are presented by section, and the ISBN-13 for each title (where appropriate) is the most current as of November 2024.

Books

"A Contemporary Story about Bullying, Broken Friendships, Social Media, and the Failures of Communication between Kids" – by John David Anderson: [978-0062338204].

"Anti-Bullying Book for Girls: Practical Tools to Manage Bullying and Build Confidence" – by Jessica Wood: This standout among bullying books for kids will help girls find their voice and put a stop to bullying, whether it's happening to them or their friends [978-1638079118].

"Artificial Intelligence: A Very Short Introduction" by Boden, M. A. (2018): Oxford. ISBN: 978-0199602919.

"Critical Thinking, Logic & Problem Solving: The Complete Guide to Superior Thinking, Systematic Problem Solving, Making Outstanding Decisions, and Uncover Logical Fallacies Like a Pro," Neurowaves Labs: [979-8866530397].

"Dear Bully: Seventy Authors Tell Their Stories" – by Metcalf, D. Dear Bully includes resources for teens, educators, and parents, and provides suggestions for further reading. For those working to support social and emotional learning and anti-bullying programs, Dear Bully can help foster reflection and empathy [978-0062060976].

"Developing Mentoring and Coaching Relationships in Early Care and Education: A Reflective Approach (Practical Resources in ECE)" – by Marilyn Chu: It is the ideal resource for anyone charged with guiding teachers, as they encounter real-world challenges in today's early childhood programs [978-0132658232].

"Digital Citizenship in Schools: Nine Elements All Students Should Know," 3rd Edition, – by Ribble, M., October 21, 2015: [978-1564843647].

"Disconnected: How to Protect Your Kids from the Harmful Effects of Device Dependency" – by Thomas Kersting: [978-1540900302].

"Eesha and the Mud Monster Mystery" – by Goucher, W. Join Eesha's cyber adventure to protect children from texting bullying (ages 7–11) [978-1915641175].

"Good Pictures Bad Pictures: Porn-Proofing Today's Young Kids," – by Jenson, K.: A comfortable way to talk with kids about pornography so your child will never be caught off guard by disturbing videos or peer pressure [978-0997318739].

"Growth Mindset Workbook for Kids: 55 Fun Activities to Think Creatively, Solve Problems, and Love Learning (Health and Wellness Workbooks for Kids)" – by Peyton Curley: A growth mindset means practicing flexible thinking and looking at challenges as opportunities to learn and grow! Discover the power of a growth mindset with hands-on activities for ages 8–12 [978-1646117031].

"Heutagogy and Lifelong Learning: A Review of Heutagogical Practice and Self-Determined Learning," Blaschke, L. M., January 2012: Oldenburg University and University of Maryland University College (UMUC), www.irrodl.org/index.php/irrodl/article/view/1076/2087.

"Hold On to Your Kids: Why Parents Need to Matter More Than Peers" – by Gordon Neufeld and Gabor Mate, M.D.: [978-0375760280].

"How to Raise Healthy Gamers: End Power Struggles, Break Bad Screen Habits, and Transform Your Relationship with Your Kids" – by Alok Kanojia, M.D., M.P.H.: [978-0593582046].

"How to Win Friends and Influence People for Teen Girls" (Dale Carnegie Books) – by Donna Dale Carnegie: Based on the beloved classic by Dale Carnegie, it has become the go-to guidebook for girls during the difficult teenage years. In these pages, teen girls get invaluable, concrete advice about the most powerful ways to influence others, defuse arguments, admit mistakes, and make self-defining choices. The Carnegie techniques promote clear and constructive communication, praise rather than criticism, emotional sensitivity, empathy, tolerance, and an optimistic outlook in every situation [978-1982149031].

"Kids' Brains & Screens: A ScreenStrong Student Course" – by Hemp, M.: Childhood screen addiction, anxiety, and mental health issues are a pressing concern for teens today, sparking meltdowns and daily battles at home and in the classroom [979-8879631845].

"Make Your Brain Work" – by Amy Brann. While this book is not for the third- and fourth-grade students, it is a helpful tool for teachers and leaders to understand the latest insights from neuroscience about how our mind works [978-1789660494].

"Oh No … Hacked Again! A Story about Online Safety" – by Zinet Kamal: While enjoying the adventures of online games, Elham struggles with making the safest decisions [978-1737775911].

"Online Safety for Children and Teens on the Autism Spectrum: A Parent's and Care's Guide" – by Nicola Lonie. While this is more of a guide for parents and caregivers, it offers valuable insights and strategies that can be translated into simpler concepts for young children [978-1849054425].

"Once Upon a Digital Story" – by Amanda Hovious. This book is designed to help children learn to tell their own stories safely and creatively online [978-1516553341].

"Security Awareness Design in the New Normal Age" – by Wendy Goucher: People working in our cyber world have access to a wide range of information including sensitive personal or corporate information which increases the risk of it. This book will primarily consider that the knowledge about secure practice is not only understood and remembered but also reliably put into practice — even when a person is working alone [Kindle ASIN - B0B1W1Z9LB].

"Taming the Machine: Ethically Harness the Power of AI" – by Nell Watson: This book offers practical insights on how you can ethically innovate with artificial intelligence (AI). It delves into the ethical issues of unbridled AI, highlighting the challenges that it will bring to society and business unless society fortifies cybersecurity, safeguards data, and understands the dangerous potential of AI [978-1398614321].

"The Anxious Generation: How the Great Rewiring of Childhood Is Causing an Epidemic of Mental Illness" – by Jonathan Haidt: In The Anxious Generation, the author explains the major causes of the international epidemic of mental illness that hit adolescents in the early 2010s and offers a path forward for parents, teachers, friends, and relatives who want to help improve the mental health of children and adolescents [978-0593655030].

"The Buzz About Social Media: A Cyber Safety Workbook and Discussion Guide for Pre-Teens, Ages 8–12" – by Shawn Marie Edgington and Emily Scheinberg: The Buzz About Social Media was created to guide you through important discussions and activities related to cyber safety and proper online behavior. This workbook is filled with suggestions, real-life situations, and activities to help you discuss the best practices for cyber safety with your children and students [978-1466495210].

"The Coddling of the American Mind: How Good Intentions and Bad Ideas are Setting up a Generation for Failure" – by Greg Lukianoff and Jonathan Haidt: The authors show how the new problems on campus have their origins in three terrible ideas that have become increasingly woven into American childhood and education [978-0735224896].

"The Digital Citizenship Handbook for School Leaders: Fostering Positive Interactions Online" – by Mike Ribble and Marty Park: Aimed at educators, this book contains valuable resources that can be adapted into lesson plans for young students [978-1564847829].

"The No More Bullying Book for Kids: Become Strong, Happy, and Bully-Proof" by Vanessa Green Allen, MEd, NBCT. This engaging book gives kids the information they need to identify bullying, followed by strategies for dealing with specific situations when they or someone they know is being bullied [978-1641520713].

"The Opt-Out Family: How to Give Your Kids What Technology Can't" – by Erin Loechner: a former social media influencer. The Opt-Out Family is packed with eye-opening research and startling insights, as well as practical encouragement and creative ideas to transform your family's relationship with today's ever-evolving technology. "It's time to reclaim your home and build a tech-free family culture that's stronger than your Wi-Fi signal" [978-0310345695].

"Killer Underwear Invasion!: How to Spot Fake News, Disinformation & Conspiracy Theories. Misinformation and Disinformation Are Everywhere" – by Elise Gravel: This book helps parents and educators assist kids learn how to navigate the confusing, modern media landscape [978-1797214917].

"Who's Raising the Kids?: Big Tech, Big Business, and the Lives of Children" – by Susan Linn: A readable social critique and guide to protecting kids from exploitation by the tech, toy, and entertainment industries [978-1620972274].

"Young Native Activist: Growing Up in Native American Rights Movements" (Young Native Boy Series Book 1) – by Aslan Tudor: Learn about activism and how young children have a voice through young Aslan's true story [978-1074524746].

"You Go First" – by Erin Entrada Kelly. An exploration of family, bullying, word games, art, and the ever-complicated world of middle school friendships [978-0062414199].

"Young Water Protectors: A Story About Standing Rock" (Young Native Boy Series Book 2) – by Aslan Tudor: Read about the author's inspiring experiences in the Oceti Sakowin Camp at Standing Rock [978-1723305689].

Articles, Research, and Whitepapers (by Lead Author)

Akgun, S., & Greenhow, C., 2022. "Artificial Intelligence in Education: Addressing Ethical Challenges in K-12 Settings," *AI Ethics*, 2, 431–440. https://doi.org/10.1007/s43681-021-00096-7.

Anderson, M., Faverio, M., & Gottfried, J., 2023. "Teens, Social Media and Technology," Pew Research Center. pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023.

Anitha, F. S., Narasimhan, U., Janakiraman, A., Janakarajan, N., & Tamilselvan, P. 2021. "Association of Digital Media Exposure and Addiction with Child Development and Behavior: A Cross-Sectional Study," *Indian Journal of Psychiatry*, 30, 265–271. https://doi.org/10.4103/ipj.ipj_157_20.

Borajy, S., Albkhari, D., Turkistani, H., Altuwairiqi, R., et al., 2019. "Relationship of Electronic Device Usage with Obesity and Speech Delay in Children," *Family Medicine & Primary Care Review,* 21, 93–97. https://doi.org/10.5114/fmpcr.2019.84542.

Bryant, J., Heitz, C., Sanghvi, S., & Wagle, D., January 14, 2020, "How Artificial Intelligence will Impact K—12 Teachers," McKinsey. https://www.mckinsey.com/industries/education/ourinsights/how-artificial-intelligence-will-impact-k-12-teachers.

Celik, I., Dindar, M., Muukkonen, H., & Järvelä, S., 2022, "The Promises and Challenges of Artificial Intelligence for Teachers: A Systematic Review of Research," *TechTrends*, 66, 616–630. https://doi.org/10.1007/s11528-022-00715-y.

Department for Culture, Media and Sport, 2018, "Disinformation and 'fake news': Interim Report," UK Parliament. https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm.

Dieterle, E., Dede, C., & Walker, M., 2022, "The Cyclical Ethical Effects of Using Artificial Intelligence in Education," *AI & Society*. https://link.springer.com/article/10.1007/s00146-022-01497-w.

Domoff, S. E., Borgen, A. L., & Radesky, J. S., 2020, "Interactional Theory of Childhood Problematic Media Use," *Human Behavior and Emerging Technologies*, 2, 343–353. https://doi.org/10.1002/hbe2.217.

Dong, C., & Mertala, P., 2021, "Preservice Teachers' Beliefs about Young Children's Technology Use at Home," *Teaching and Teacher Education*, 102, 103325. https://doi.org/10.1016/j.tate.2021.103325.

Doyle, C., Douglas, E., & O'Reilly, G., 2021, "The Outcomes of Sexting for Children and Adolescents: A Systematic Review of the Literature," *Journal of Adolescence*, 92, 86–113. sciencedirect.com/science/article/pii/S0140197121001111.

Ehrenreich, S. E., Beron, K. J., Burnell, K., Meter, D. J., & Underwood, M. K., 2020, "How Adolescents Use Text Messaging Through Their High School Years," *Journal of Research on Adolescence*, 30(2), 521–540. https://doi.org/10.1111/jora.12541.

European Commission, Directorate-General for Education, Youth, Sport and Culture, 2022, Ethical guidelines on the use of artificial intelligence (AI) and data in teaching and learning for educators. Publications Office of the European Union. https://data.europa.eu/doi/10.2766/153756.

Faverio, M., 2024, "Teens and Social Media Fact Sheet," Pew Research Center, pewresearch.org/internet/fact-sheet/teens-and-social-media-fact-sheet/?tabId=tab-7c5235eb-c885-4465-9eb2-6d1cf388423b.

Forsyth, S., Dalton, B., Foster, E. H., Walsh, B., Smilack, J., & Yeh, T., 2021, May, "Imagine a more Ethical AI: Using Stories to Develop Teens' Awareness and Understanding of Artificial Intelligence and Its Societal Impacts", In *2021 Conference on Research in Equitable and Sustained Participation in Engineering, Computing, and Technology (RESPECT)*. IEEE. https://doi.org/10.1109/RESPECT51740.2021.9620549.

Hinduja, S., October 21, 2021, “Cyberbullying Statistics 2021: Age, Gender, Sexual Orientation, and Race,” Cyberbullying Research Center, cyberbullying.org/cyberbullying-statistics-age-gender-sexual-orientation-race.

Hinduja, S., & Patchin, J. W., 2022, “Teen Sexting: A Brief Guide for Educators and Parents,” Cyberbullying Research Center, cyberbullying.org/sexting-research-summary-2022.pdf.

Hutton, J. S., Huang, G., Sahay, R. D., DeWitt, T., & Ittenbach, R. F., 2020, “A Novel, Composite Measure of Screen-Based Media Use in Young Children (Screen Q) and Associations with Parenting Practices and Cognitive Abilities,” *Pediatric Research*, 87, 1211–1218. https://doi.org/10.1038/s41390-020-0765-1.

IEEE-USA Board of Directors, February 10, 2017, “Artificial Intelligence Research, Development, and Regulation,” IEEE. http://globalpolicy.ieee.org/wp-content/uploads/2017/10/IEEE17003.pdf.

International Society for Technology in Education [ISTE], 2016, “Digital Citizenship Defined: Teach the 9 Elements to Enhance Students’ Safety, Creativity and Empathy,” https://cdn2.hubspot.net/hubfs/1818747/Images/Marketing%20Campaigns/Digital%20Citizenship/Digital_Citizenship_Downloadable_10-2016_v11_web.pdf.

Khan, F., Limbana, T., Zahid, T., Eskander, N., & Jahan, N., August 2022, “Traits, Trends, and Trajectory of Tween and Teen Cyberbullies,” *Cureus*, 12(8), e9738. https://doi.org/10.7759/cureus.9738. PMID: 32821629; PMCID: PMC7430539.

Khosravi, H., Shum, S. B., Chen, G, Conati, C., Tsai, Y-S., Kay, J., Knight, S., Martinez-Maldonado, R., Sadiq, S., & Gašević, D., 2022, “Explainable Artificial Intelligence in Education,” *Computers and Education: Artificial Intelligence*, 3. https://doi.org/10.1016/j.caeai.2022.100074.

Klein, A., May 10, 2023, “AI Literacy, Explained, Education Wek,” https://drive.google.com/file/d/1k0v1UddIK4PoijF763CV5mKG7x3cN-2-/view.

Kreski, N. T., Chen, Q., Olfson, M., Cerdá, M., Martins, S. S., … Keyes, K. M., 2022, “Experiences of Online Bullying and Offline Violence-Related Behaviors Among a Nationally Representative Sample of U.S. Adolescents, 2011 to 2019,” *Journal of School Health*. https://doi.org/10.1111/josh.13144.

Lenhart, A., Anderson, M., & Smith, A., October 2015, “Teens, Technology and Romantic Relationships,” Pew Research Center, assets.pewresearch.org/wp-content/uploads/sites/14/2015/10/PI_2015-10-01_teens-technology-romance_FINAL.pdf.

Lykens, J., Pilloton, M., Silva, C., Schlamm, E., & Sheoran, B., 2017, “TECHsex: Youth Sexuality and Health Online,” YTH, yth.org/wp-content/uploads/YTH-TECHsex-2017-report.pdf.

Macapagal, K., Moskowitz, D. A., Li, D. H., Carrión, A., Bettin, E., Fisher, C. B., & Mustanski, B., 2018, “Hookup App Use, Sexual Behavior, and Sexual Health among Adolescent Men Who Have Sex with Men in the United States,” *Journal of Adolescent Health*, 62(6), 708–715. https://doi.org/10.1016/j.jadohealth.2018.01.001.

Madigan, S., Ly, A., Rash, C. L., Ouytsel, J. V., & Temple, J. R., 2018, “Prevalence of Multiple Forms of Sexting Behavior among Youth: A Systematic Review and Meta-Analysis,” *JAMA Pediatrics*, 172(4), 327–335, https://doi.org/10.1001/jamapediatrics.2017.5314.

Microsoft, 2022, “Microsoft Responsible AI Standard, v2 General Requirements,” https://blogs.microsoft.com/wp-content/uploads/prod/sites/5/2022/06/Microsoft-Responsible-AI-Standard-v2-General-Requirements-3.pdf.

Murphy, H., 2019, “Inside Facebook’s Information Warfare Team, Financial Times,” https://www.ft.com/content/70b86214-9e77-11e9-9c06-a4640c9feebb.

Öztürk, G, 2021, “Digital Citizenship and Its Teaching: A Literature Review,” *Journal of Educational Technology & Online Learning*, 4(1). https://dergipark.org.tr/en/pub/jetol/issue/60134/857904.

Patchin, J. W., October 4, 2023, “Cyberbullying Continues to Rise among Youth in the United States,” Cyberbullying Research Center, cyberbullying.org/cyberbullying-continues-to-rise-among-youth-in-the-united-states-2023.

Pennycook, G., & Rand, D. G., 2021, “The Psychology of Fake News, ScienceDirect,” www.sciencedirect.com/science/article/pii/S1364661321000516.

Piper Sandler Companies, 2024, Spring, “Taking Stock with Teens®,” pipersandler.com/teens.

Radesky, J., Weeks, H. M., Schaller, A., Robb, M., & Lenhart, A., 2023, “Constant Companion: A Week in the Life of a Young Person’s Smartphone Use,” Common Sense, commonsensemedia.org/research/constant-companion-a-week-in-the-life-of-a-young-persons-smartphone-use.

Rideout, V., & Fox, S., 2018, “Digital Health Practices, Social Media Use, and Mental Well-Being among Teens and Young Adults in the U.S. Hopelab and Well Being Trust,” assets.hopelab.org/wp-content/uploads/2020/08/a-national-survey-by-hopelab-and-well-being-tr ust-2018.pdf.

Rideout, V., Peebles, A., Mann, S., & Robb, M. B., 2022, “The Common Sense Census: Media Use by Tweens and Teens,” 2021, commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021.

Robb, M. B. & Mann, S., 2023, “Teens and Pornography,” Common Sense, commonsensemedia.org/sites/default/files/research/report/2022-teens-and-pornography-final-web.pdf.

Johnson, S., Krall, B., Mims, A., & Burstein, R., 2024. “Three Tips for Teachers – Not Tools – in Generative AI Innovation,” https://digitalpromise.org/2024/09/17/three-tips-for-centering-teachers-not-tools-in-generative-ai-innovation/

Sawyer, A. N., Smith, E. R., & Benotsch, E. G., 2018, “Dating Application Use and Sexual Risk Behavior among Young Adults,” *Sexuality Research and Social Policy*, 15(2), 183–191, https://doi.org/10.1007/s13178-017-0297-6.

Stephanidis, C., Salvendy, G., Chen, J. Y. C., Dong, J., et al., 2019, “Seven HCI Grand Challenges,” *International Journal of Human–Computer Interaction*, 35(14), 1229–1269, https://doi.org/10.1080/10447318.2019.1619259, www.tandfonline.com/doi/epdf/10.1080/10447318.2019.1619259?needAccess=true.

Strasburger, V. C., Zimmerman, H., Temple, J. R., & Madigan, S., 2019, “Teenagers, Sexting, and the Law,” *Pediatrics*, 143(5), e20183183, https://doi.org/10.1542/peds.2018-3183.

Swiecki, Z., Khosravi, H., Chen, G., Martinez-Maldonado, R., Lodge, J. M., Milligan, S., Selwyn, B. & Gašević, D., 2022, “Assessment in the Age of Artificial Intelligence,” *Computers and Education: Artificial Intelligence*, 3. https://doi.org/10.1016/j.caeai.2022.100075.

The White House Office of Science and Technology Policy, October 2022, “Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People. The White House Office of Science and Technology Policy,” https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/

Tienda, M., Goldberg, R. E., & Westreich, J. R., 2022, “Adolescents’ Partner Search in the Digital Age: Correlates and Characteristics of Relationships Initiated Online,” *Journal of Youth and Adolescence*, 51, 393–498, https://doi.org/10.1007/s10964-021-01557-2.

Vateraus, J. M., Tulane, S., Porter, B. D., & Beckert, T. E., 2018, “The Perceived Influence of Media and Technology on Adolescent Romantic Relationships,” *Journal of Adolescent Research*, 33(6), 651–671, https://doi.org/10.1177/0743558417712611.

White, S., Scott, A., Koshy, S., January 18, 2024, “Responsible AI & Tech Justice: A Guide for K—12 Education,” Kapor Foundation, https://kaporfoundation.org/wp-content/uploads/2024/01/Responsible-AI-Guide-Kapor-Foundation.pdf.

Zhang, H., Lee, I., Ali, S., DiPaola, D., Cheng, Y., & Breazeal, C., 2022, “Integrating Ethics and Career Futures with Technical Learning to Promote AI Literacy for Middle School Students: An Exploratory Study,” *International Journal of Artificial Intelligence in Education*, 1–35. https://doi.org/10.1007/s40593-022-00293-3.

Appendix C: Social Media/Networking

Additional Information for Educators and Parents

Social Media: Refers to platforms where users create, share, and consume content such as photos, videos, and articles. Examples include Instagram, TikTok, and YouTube.

Social Networking: Involves platforms where the primary focus is on building and maintaining personal and professional relationships. Examples include Facebook, LinkedIn, and Twitter.

Understanding these differences helps parents and educators guide children and teens in using these platforms appropriately. Social media can expose users to a wide range of content, including inappropriate material, while social networking focuses more on interactions, which can involve privacy concerns and potential cyberbullying. Awareness allows for better monitoring and setting appropriate boundaries for safe and responsible usage.

As with any compiled list that examines technology, especially technology changing as rapidly as websites and apps, this Appendix is current as of November 2024.

While every effort is made to provide accurate, complete, and secure information, it is important to acknowledge that no guarantees can be given regarding the accuracy, completeness, or security of websites that may be accessed by the reader. The viability of external websites is beyond the control of the authors, and their content, availability, and security may vary. Readers are encouraged to exercise caution and to verify information independently when relying on external sources.[1]

The opinions expressed in any of these third-party materials included as references or examples do not necessarily reflect the positions or policies of the authors or the publisher.

Websites

These websites provide various resources and tools to help parents, guardians, and educators ensure the online safety and appropriate use of technology by children and young people.

WEBSITE NAME	WEBSITE URL
AskAboutGames	www.askaboutgames.com
Be internet awesome	https://beinternetawesome.withgoogle.com
Better internet for kids	www.betterinternetforkids.eu
Childnet	www.childnet.com
Children & young people	https://hillingdonsafeguardingpartnership.org.uk/children-and-young-people/
Common sense media	www.commonsensemedia.org
Cyberwise	www.cyberwise.org
Digital citizenship	www.digitalcitizenship.net
DigiParenting	www.digital-parenting.com/
Education.com	www.education.com
Educate empower kids	www.educateempowerkids.org
Ensuring a safe digital playground: Websites and apps for children	https://medium.com/@alushaks/ensuring-a-safe-digital-playground-websites-and-apps-for-children-546693d80b0f
ESRB	www.esrb.org
Family online safety institute	www.fosi.org
Get safe online	www.getsafeonline.org
Google family link	https://families.google.com/familylink
HealthyChildren.org	www.healthychildren.org
Hillingdon safeguarding partnership	www.hillingdonsafeguardingpartnership.org.uk
Internet matters	www.internetmatters.org
iParenting	www.iparentinglife.com
Kiddle	www.kiddle.co
Kids in mind	www.kids-in-mind.com
KidsHealth	www.kidshealth.org
KidRex	www.alarms.org/kidrex/
KidZui	www.kidzui.com
Mental health America	www.mhanational.org/websites-and-apps-be-aware-cheat-sheet-parents
Net nanny	www.netnanny.com
NetSmartz	www.missingkids.org/netsmartz
Norton family	https://us.norton.com/norton-family-premier
NSPCC	www.nspcc.org.uk
Online sense	www.onlinesense.org
Parent zone	www.parentzone.org.uk
Protect young eyes	www.protectyoungeyes.com
Safe search kids	www.safesearchkids.com
Safe teens	www.safeteens.org
Safekids.com	www.safekids.com

(*Continued*)

(***Continued***)

WEBSITE NAME	WEBSITE URL
Safer internet	www.saferinternet.org.uk
Smart social	www.smartsocial.com
Social media cheat sheet—mental health America	https://mhanational.org/youth-tech/social-media-cheat-sheet
SmartSocial.com	https://smartsocial.com/app-guide-parents-teachers
Stay safe online	www.staysafeonline.org
StopBullying.gov	www.stopbullying.gov
Super smart kids	www.supersmartkids.com
Surfnetkids	www.surfnetkids.com
TeenSafe	www.teensafe.net/
UK safer internet centre	www.saferinternet.org.uk
Webwise	www.webwise.ie
Wired safety	https://www.iacpcybercenter.org/labs/wiredsafety-2/
YouTube kids	https://kids.youtube.com
Zift	https://wezift.com
Zoodles	www.zoodles.com
ZoneAlarm	www.zonealarm.com
Zoo.com	www.zoo.com

App Websites

In the technology, Internet, and online environment, “app” stands for “application.” An app is a software program designed to perform specific tasks or functions on devices such as smartphones, tablets, and computers. Apps can range from simple tools and utilities to complex programs and games, providing users with a wide variety of functionalities and services.

The following websites analyze, evaluate, rank, and rate apps based on the safety of use by children, young adults, tweens, and teens.

WEBSITE NAME	WEBSITE URL
App advice	https://appadvice.com/home
App annie	www.appannie.com
App review central	www.appreviewcentral.net
Appolicious	www.appolicious.com
AppleVis	www.applevis.com
AppSmitten	www.appsmitten.com
Children’s technology review	www.reviews.childrenstech.com/ctr/home.php
Common sense media	www.commonsensemedia.org
Cynopsis kids	www.cynopsis.com/cynopsis-kids
Digital trends	www.digitaltrends.com
Educational app store	www.educationalappstore.com
Edutopia	www.edutopia.org

(*Continued*)

(***Continued***)

WEBSITE NAME	WEBSITE URL
Family app guide	www.familyappguide.com
Family online safety institute	www.fosi.org
GeekDad	www.geekdad.com
Good app guide	www.goodappguide.com
Google play parental controls	www.support.google.com/googleplay/answer/1075738?hl=en
iMore	www.imore.com
KidzVuz	www.kidzvuz.com
Learningworks for kids	www.learningworksforkids.com
Little pickle press	www.littlepicklepress.com
MakeUseOf	www.makeuseof.com
Mashable	www.mashable.com
Moshi monsters	www.moshimonsters.com
Mumsnet	www.mumsnet.com
My kids' adventures	www.mykidsadventures.com
National online safety	www.nationalonlinesafety.com
Net nanny	www.netnanny.com
Norton family	https://us.norton.com/feature/parental-control
Parenting	www.parenting.com
Parents' choice	www.parents-choice.org
PCMag	www.pcmag.com
Pocket-lint	www.pocket-lint.com
Protect young eyes	www.protectyoungeyes.com
Safe smart social	www.safesmartsocial.com
SafeKids	www.safekids.com
Safer internet	www.saferinternet.org.uk
Smart social	www.smartsocial.com
TechCrunch	www.techcrunch.com
The toy insider	www.thetoyinsider.com
Toca boca	www.tocaboca.com
Wee society	www.weesociety.com

Risky Apps

These apps are known for having potential risks that can expose children, young adults, tweens, and teens to inappropriate content such as…, cyberbullying, privacy concerns, and predatory behavior. Parents, guardians, and educators must be aware of these risks and can monitor app usage through such appropriate software.

APP NAME	DESCRIPTION	RISK OR EXPOSURE
AfterSchool	An anonymous app for high school students to share content	Cyberbullying, inappropriate content
Ask.fm	A social networking site where users ask each other questions	Cyberbullying, anonymity leading to harassment

(*Continued*)

(***Continued***)

APP NAME	DESCRIPTION	RISK OR EXPOSURE
Badoo	A dating-focused social network	Inappropriate content, potential for predatory behavior
BIGO Live	A live streaming app	Inappropriate content, exposure to strangers
BitLife	A life simulation game	Inappropriate content, mature themes
Blendr	A location-based dating app	Inappropriate content, potential for predatory behavior
Burnbook	An anonymous posting app	Cyberbullying, hate speech
Calculator%	A secret photo vault disguised as a calculator	Hidden content, potential for sexting
CapCut	A creative video editor	Potential for predatory behavior through chat
Chatroulette	A video chat platform	Exposure to inappropriate content, strangers
Discord	A chat app for gamers	Inappropriate content, cyberbullying
Foursquare	A location-sharing social network	Privacy concerns, potential for stalking
Grindr	A dating app for LGBTQ+ users	Inappropriate content, potential for predatory behavior
Houseparty	A group video chat app	Inappropriate content, privacy concerns
Holla	A live video chat app	Exposure to inappropriate content, strangers
Hoop	A Snapchat friend discovery app	Inappropriate content, potential for predatory behavior
Hot or not	A social app for rating profiles	Inappropriate content, cyberbullying
IMVU	A virtual world and social network	Inappropriate content, potential for predatory behavior
Kik	A messaging app	Inappropriate content, potential for predatory behavior
Likee	A video creation and sharing app	Inappropriate content, exposure to strangers
Live.me	A live streaming app	Inappropriate content, exposure to strangers
LoL jokes	An anonymous joke-sharing app	Inappropriate content, cyberbullying
MeetMe	A social discovery app	Inappropriate content, potential for predatory behavior
MeWe	A social networking app	Inappropriate content, lack of moderation
Monkey	A live video chat app	Inappropriate content, exposure to strangers
Mocospace	A mobile social network	Inappropriate content, potential for predatory behavior
Omegle	A chat site that pairs users with strangers	Inappropriate content, exposure to strangers
Periscope	A live video streaming app	Inappropriate content, exposure to strangers
Poparazzi	A social media app for candid photos	Inappropriate content, privacy concerns
Reddit	A social news aggregation site	Inappropriate content, lack of moderation
Roblox	Online multiplayer gaming platform	Inappropriate content, exposure to strangers, cyberbullies, hackers, online predators
Sarahah	An anonymous messaging app	Cyberbullying, harassment
SayAt.Me	An anonymous Q&A app	Cyberbullying, harassment
Scout	A location-based dating app	Inappropriate content, potential for predatory behavior
Secret	An anonymous social network	Cyberbullying, harassment
SimSimi	An AI chatbot app	Inappropriate content, offensive language
Skout	A location-based dating app	Inappropriate content, potential for predatory behavior
Snapchat	A multimedia messaging app	Inappropriate content, privacy concerns
Spotafriend	A friend discovery app	Inappropriate content, potential for predatory behavior
Steam Chat	A chat app for gamers	Inappropriate content, cyberbullying
Tango	A live streaming app	Inappropriate content, exposure to strangers
Telegram	A messaging app	Inappropriate content, lack of moderation
TikTok	A video-sharing social network	Inappropriate content, privacy concerns
Tinder	A dating app	Inappropriate content, potential for predatory behavior
Topface	A dating-focused social network	Inappropriate content, potential for predatory behavior
Tumblr	A microblogging and social networking site	Inappropriate content, lack of moderation

(*Continued*)

(***Continued***)

APP NAME	DESCRIPTION	RISK OR EXPOSURE
Voxer	A walkie-talkie-style messaging app	Inappropriate content, potential for predatory behavior
WhatsApp	A messaging app	Inappropriate content, privacy concerns
Whisper	An anonymous social network	Cyberbullying, inappropriate content
Yubo	A social discovery app	Inappropriate content, potential for predatory behavior
Yik Yak	An anonymous social media app	Cyberbullying, harassment
YouNow	A live streaming app	Inappropriate content, exposure to strangers

Questionable Apps

While these apps are not outright risky, they pose potential risks and exposures to children, young adults, tweens, and teens. Their installation and use on mobile devices should be closely monitored by parents, caregivers, trusted adults, and when and where appropriate, by educators.

APP NAME	DESCRIPTION	RISK OR EXPOSURE
AfterSchool	Anonymous app for high school students	Cyberbullying, inappropriate content
Amino	Interest-based social network	Inappropriate content, potential for predatory behavior
Ask.fm	Anonymous Q&A app	Cyberbullying, anonymity leading to harassment
BeReal	Allows kids to post a photo once a day that will be shared with friends they're linked to	Posts don't appear to be screened
BIGO live	Live streaming app	Inappropriate content, exposure to strangers
BitLife	Life simulation game	Inappropriate content, mature themes
Blendr	Location-based dating app	Inappropriate content, potential for predatory behavior
Bumble	Dating app	Inappropriate content, potential for predatory behavior
Burnbook	Anonymous posting app	Cyberbullying, hate speech
Calculator%	Secret photo vault disguised as a calculator	Hidden content, potential for sexting
Chatroulette	Video chat platform	Exposure to inappropriate content, strangers
Discord	Chat app for gamers	Inappropriate content, cyberbullying
Foursquare	Location-sharing social network	Privacy concerns, potential for stalking
Grindr	Dating app for LGBTQ+ users	Inappropriate content, potential for predatory behavior
HOLLA	Live video chat app	Exposure to inappropriate content, strangers
Houseparty	Group video chat app	Inappropriate content, privacy concerns
Huggle	Location-based social app	Privacy concerns, potential for predatory behavior
IMVU	Virtual world and social network	Inappropriate content, potential for predatory behavior
Kik	Messaging app	Inappropriate content, potential for predatory behavior
Likee	Video creation and sharing app	Inappropriate content, exposure to strangers
Live.me	Live streaming app	Inappropriate content, exposure to strangers
LOVOO	Dating app	Inappropriate content, potential for predatory behavior
MeetMe	Social discovery app	Inappropriate content, potential for predatory behavior
Monkey	Live video chat app	Inappropriate content, exposure to strangers
Omegle	Chat site with strangers	Inappropriate content, exposure to strangers
Periscope	Live video streaming app	Inappropriate content, exposure to strangers

(*Continued*)

(*Continued*)

APP NAME	DESCRIPTION	RISK OR EXPOSURE
Poparazzi	Social media app for candid photos	Inappropriate content, privacy concerns
Reddit	Social news aggregation site	Inappropriate content, lack of moderation
Sarahah	Anonymous messaging app	Cyberbullying, harassment
SayAt.Me	Anonymous Q&A app	Cyberbullying, harassment
Scout	Location-based dating app	Inappropriate content, potential for predatory behavior
Secret	Anonymous social network	Cyberbullying, harassment
SimSimi	AI chatbot app	Inappropriate content, offensive language
Skout	Location-based dating app	Inappropriate content, potential for predatory behavior
Snapchat	Multimedia messaging app	Inappropriate content, privacy concerns
Spotafriend	Friend discovery app	Inappropriate content, potential for predatory behavior
Steam chat	Chat app for gamers	Inappropriate content, cyberbullying
Tango	Live streaming app	Inappropriate content, exposure to strangers
Telegram	Messaging app	Inappropriate content, lack of moderation
TikTok	Video-sharing social network	Inappropriate content, privacy concerns
Tinder	Dating app	Inappropriate content, potential for predatory behavior
Topface	Dating-focused social network	Inappropriate content, potential for predatory behavior
Tumblr	Microblogging and social networking site	Inappropriate content, lack of moderation
Viber	Messaging app	Inappropriate content, privacy concerns
Voxer	Walkie-talkie style messaging app	Inappropriate content, potential for predatory behavior
WeChat	Messaging and social media app	Privacy concerns, potential for predatory behavior
WhatsApp	Messaging app	Inappropriate content, privacy concerns
Whisper	Anonymous social network	Cyberbullying, inappropriate content
Wink	Friend discovery app	Inappropriate content, potential for predatory behavior
Yubo	Social discovery app	Inappropriate content, potential for predatory behavior
Zello	Walkie-talkie-style messaging app	Inappropriate content, potential for predatory behavior

App Monitoring Software

The following software apps provide various features to help parents, educators, and trusted adults monitor and control children's web and app activity, ensuring a safer online experience.

APP NAME	DESCRIPTION	URL
Bark	Monitors texts, emails, social media, and provides alerts for potential issues	www.bark.us/bark-phone/
Boomerang	Monitors app usage, sets screen time limits, and tracks location	www.useboomerang.com
Circle home plus	Manages screen time, filters content, and monitors usage across all devices	www.meetcircle.com
Clean router	Filters and logs Internet activity, blocks inappropriate content	www.cleanrouter.com
Covenant eyes	Tracks Internet use and provides accountability reports	www.covenanteyes.com
Custodio	Monitors social media, web activity, and sets screen time limits	www.custodio.com
ESET parental control	Monitors app usage, sets screen time limits, and filters web content	www.eset.com
FamilyTime	Tracks location, sets screen time limits, and blocks apps	www.familytime.io

(*Continued*)

(***Continued***)

APP NAME	DESCRIPTION	URL
Family orbit	Tracks location, monitors texts and calls, and sets screen time limits	www.familyorbit.com
FlexiSPY	Monitors texts, calls, and social media activity	www.flexispy.com
Highster mobile	Monitors texts, calls, GPS location, and social media activity	www.highstermobile.com
Intego ContentBarrier	Monitors Internet usage and blocks inappropriate content	www.intego.com
Kaspersky safe kids	Monitors app usage, tracks location, and sets screen time limits	www.kaspersky.com
KidLogger	Tracks keystrokes, app usage, and web activity	www.kidlogger.net
Kidslox	Manages screen time, blocks apps, and sets usage schedules	www.kidslox.com
MamaBear	Monitors social media, tracks location, and provides driving reports	www.mamabearapp.com
McAfee safe family	Tracks location, sets time limits, and blocks apps	www.mcafee.com
Mobicip	Filters content, monitors usage, and sets screen time limits	www.mobicip.com
mSpy	Monitors texts, calls, GPS location, and social media activity	www.mspy.com
Net nanny	Filters web content, monitors social media, and sets time limits	www.netnanny.com
Norton family	Monitors web activity, sets time limits, and tracks location	www.norton.com
OurPact	Blocks apps, sets screen time limits, and monitors activity	www.ourpact.com
PhoneSheriff	Monitors texts, calls, GPS location, and sets time limits	www.phonesheriff.com
Qustodio	Monitors web activity, blocks apps, and sets time limits	www.qustodio.com
ReThink	Detects and alerts for offensive language in texts and social media	www.rethinkwords.com
Safe lagoon	Monitors app usage, tracks location, and sets time limits	www.safelagoon.com
SafeDNS	Filters web content and monitors Internet usage	www.safedns.com
SafeToNet	Filters harmful content, provides real-time alerts, and offers parental controls	www.safetonet.com
Screen time labs	Sets screen time limits, monitors app usage, and provides daily reports	www.screentimelabs.com
Securly home	Monitors online activity, filters content, and tracks location	www.securly.com/home
SecureTeen	Monitors texts, calls, GPS location, and social media activity	www.secureteen.com
SentryPC	Tracks keystrokes, monitors usage, and blocks websites	www.sentrypc.com
Silent phone	Encrypts calls and messages, ensuring privacy	www.silentcircle.com
Spyera	Monitors texts, calls, GPS location, and social media activity	www.spyera.com
Spyic	Monitors texts, calls, GPS location, and social media activity	www.spyic.com
Surfie	Monitors app usage, blocks inappropriate content, and tracks location	www.surfie.com
TheOneSpy	Monitors texts, calls, GPS location, and social media activity	www.theonespy.com
uKnowKids	Monitors social media, texts, and provides alerts for potential issues	www.uknowkids.com
WebWatcher	Monitors texts, calls, GPS location, and social media activity	www.webwatcher.com
Wondershare famisafe	Tracks location, sets geofences, and monitors app usage	https://famisafe.wondershare.com/
Xnspy	Monitors texts, calls, GPS location, and social media activity	www.xnspy.com
YouTube kids	Provides child-friendly content and allows parents to set usage limits	https://www.youtube.com/kids/familyfriendly-videos/
Zift	Monitors app usage, filters content, and sets screen time limits	www.wezift.com

Research

The following is a list of relevant social media/networking research sources. These research sources address the topics of social media safety and the impact of social media on young adults.

Keeping Safe

Higgin, T., September 16, 2022, “Keeping Your Students (and Yourself) Safe on Social Media: A Checklist: Learn How to Keep Personal Information Confidential on Social Media,” Common Sense, www.commonsense.org/education/articles/keeping-your-students-and-yourself-safe-on-social-media-a-checklist.

Family Media Plan—American Academy of Pediatrics
Since media habits are different for every household, the Family Media Plan can be customized to meet individual family’s needs. Make a full plan, or just choose a few parts that matter the most to your family.
www.healthychildren.org/MediaUsePlan.

Teens, Social Media and Technology, 2023, www.pewresearch.org/internet/2023/12/11/teens-social-media-and-technology-2023/

15 Apps Parents Should Know About.
https://x.com/PSLPolice/status/1181028222668087296.

Youth Mental Health

Social Media and Youth Mental Health
(sources listed alphabetically by author)

Allcott, H., Gentzkow, M., & Song, L., 2022, “Digital Addiction,” *American Economic Review*, 112(7), 2424–2463, https://doi.org/10.1257/aer.20210867.

American Academy of Pediatrics, February 7, 2023. “Center of Excellence on Social Media and Youth Mental Health,” www.aap.org/en/patient-care/media-and-children/center-of-excellence-on-social-media-and-youth-mental-health/#:~:text=What%20We%20Do,protect%20 youth%20mental%20health%20online.

American Psychological Association, 2023, “Health Advisory on Social Media Use in Adolescence,” American Psychological Association, www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use. pdf.

Bickham, D. S., Hunt, E., Bediou, B., & Rich, M., 2022, *Adolescent Media Use: Attitudes, Effects, and Online Experiences*. Boston, MA: Boston Children’s Hospital Digital Wellness Lab, https://digitalwellnesslab.org/wp-content/uploads/Pulse-Survey_Adolescent-Attitudes-Effects-and-Experiences.pdf.

Braghieri, L., Levy, R., & Makarin, A., 2022, “Social Media and Mental Health,” *American Economic Review*, 112(11), 3660–3693, https://pubs.aeaweb.org/doi/abs/10.1257/aer.20211218.

Carville, O., November 30, 2022. “TikTok’s Viral Challenges Keep Luring Young Kids to Their Deaths,” Bloomberg, www.bloomberg.com/news/features/2022-11-30/is-tiktok-responsible-if-kids-die-doing-dangerous-viral-challenges.

Dekkers, T. J., & van Hoorn, J., 2022, “Understanding Problematic Social Media Use in Adolescents with Attention-Deficit/Hyperactivity Disorder (ADHD): A Narrative Review and Clinical Recommendations,” *Brain Sciences*, 12(12), 1625, https://doi.org/10.3390/brainsci12121625.

Doucleff, M., April 25, 2023. “The Truth about Teens, Social Media and the Mental Health Crisis,” NPR, www.npr.org/sections/health-shots/2023/04/25/1171773181/social-media-teens-mental-health.

Dyer, C., 2022, “Social Media Content Contributed to Teenager’s Death ‘In More than a Minimal Way,’ Says Coroner,” *BMJ* (Clinical research ed.), 379, o2374, https://doi.org/10.1136/bmj.o2374.

Ehmke, R., March 13, 2023, “How Using Social Media Affects Teenagers,” Child Mind Institute. https://childmind.org/article/how-using-social-media-affects-teenagers.

Federal Bureau of Investigations, December 19, 2022, “FBI and Partners Issue National Public Safety Alert on Financial Sextortion Schemes,” FBI, www.fbi.gov/news/press-releases/fbi-and-partners-issue-national-public-safety-alert-on-financial-sextortion-schemes.

Finkelhor, D., Turner, H., & Colburn, D., 2022, “Prevalence of Online Sexual Offenses Against Children in the US,” *JAMA Network Open*, 5(10), e2234471. https://doi.org/10.1001/jamanetworkopen.2022.34471.

Finkelhor, D., Turner, H. A., & Colburn, D., 2023, “Which Dynamics Make Online Child Sexual Abuse and Cyberstalking More Emotionally Impactful: Perpetrator Identity and Images?” *Child Abuse & Neglect*, 137, 106020, https://doi.org/10.1016/j.chiabu.2023.106020.

Gelles-Watnick, R., 2022, “Explicit Content, Time-wasting are Key Social Media Worries for Parents of U.S. Teens,” Pew Research Center, United States of America, www.pewresearch.org/fact-tank/2022/12/15/explicit-content-time-wasting-are-key-social-media-worries-for-parents-of-u-s-teens/.

Kruzan, K. P., Williams, K. D. A., Meyerhoff, J., Yoo, D. W., O’Dwyer, L. C., De Choudhury, M., & Mohr, D. C., 2022, “Social Media-Based Interventions for Adolescent and Young Adult Mental Health: A Scoping Review,” *Internet Interventions*, 30, 100578. https://doi.org/10.1016/j.invent.2022.100578.

Mayo Clinic Staff, n.d., “Teens and Social Media Use: What’s the Impact?” www.mayoclinic.org/healthy-lifestyle/tween-and-teen-health/in-depth/teens-and-social-media-use/art-20474437.

Maza, M. T., Fox, K. A., Kwon, S. J., Flannery, J. E., Lindquist, K. A., Prinstein, M. J., & Telzer, E. H., 2023, “Association of Habitual Checking Behaviors on Social Media with Longitudinal Functional Brain Development,” *JAMA Pediatrics*, 177(2), 160–167. https://doi.org/10.1001/jamapediatrics.2022.4924.

Miech, R. A., Johnston, L. D., Bachman, J. G., O'Malley, P. M., Schulenberg, J. E., & Patrick, M. E., 2022, "Monitoring the Future: A Continuing Study of American Youth (8th- and 10th-Grade Surveys), 2021," Inter-University Consortium for Political and Social Research [distributor], https://doi.org/10.3886/ICPSR38502.v1.

Morgan Stanley Alliance for Children's Mental Health & Child Mind Institute, May 2022, "How to Set Limits on Screen Time and Internet Use," www. morganstanley.com/assets/pdfs/setting-limits-on-screen-time-tip-sheet.pdf.

Nesi, J., Mann, S., & Robb, M. B., 2023, *Teens and Mental Health: How Girls Really Feel about Social Media*. San Francisco, CA: Common Sense, https://www.commonsensemedia.org/research/teens-and-mental-health-how-girls-really-feel-about-social-media.

Odgers, C., Allen, N., Pfeifer, J., Dahl, R., Nesi, J., Schueller, S. M., Williams, J. L., & the National Scientific Council on Adolescence, 2022, Engaging, safe, and evidence-based: What science tells us about how to promote positive development and decrease risk in online spaces, Council Report No. 2. https://doi.org/10.31234/osf.io/rvn8q.

Odgers, C. L., Allen, N. B., Pfeifer, J. H., Dahl, R. E., Nesi, September 9, 2022, "Social Media Use and Health and Well-being of Lesbian, Gay, Bisexual, Transgender, and Queer Youth: Systematic Review," *Journal of Medical Internet Research*, 24(9), e38449, https://doi.org/10.2196/38449.

Orben, A., Przybylski, A. K., Blakemore, S. J., et al., March 28, 2022, "Windows of Developmental Sensitivity to Social Media," *Nature Communication*, 13(1649), https://doi.org/10.1038/s41467-022-29296-3.

Perrino, J., July 27, 2022, "Using 'Safety By Design' to Address Online Harms," Brookings Institute, www. brookings.edu/techstream/using-safety-by-design-to-address-online-harms/.

Rideout, V., Peebles, A., Mann, S., & Robb, M. B., 2022, *Common Sense Census: Media Use by Tweens and Teens, 2021*. San Francisco, CA: Common Sense, https://www.commonsensemedia.org/research/the-common-sense-census-media-use-by-tweens-and-teens-2021.

Shannon, H., Bush, K., Villeneuve, P. J., Hellemans, K. G., & Guimond, S., 2022, "Problematic Social Media Use in Adolescents and Young Adults: Systematic Review and Meta-Analysis," *JMIR Mental Health*, 9(4), e33450. https://doi.org/10.2196/33450.

Shafi, R. M. A., Nakonezny, P. A., Romanowicz, M., Nandakumar, A. L., Suarez, L., & Croarkin, P. E., December 29, 2019, "The Differential Impact of Social Media Use on Middle and High School Students: A Retrospective Study," *Journal of Child and Adolescent Psychopharmacology*, 29(10),746–752. https://doi.org/10.1089/cap.2019.0071. Epub June 24, 2022. PMID: 31233343, PMCID: PMC6885760, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6885760/.

Thai, H., Davis, C. G., Mahboob, W., Perry, S., Adams, A., & Goldfield, G. S., 2023, "Reducing Social Media Use Improves Appearance and Weight Esteem in Youth with Emotional Distress," *Psychology of Popular Media*. https://doi.org/10.1037/ppm0000460.

The U.S. Surgeon General, 2023, “Social Media and Youth Mental Health,” The U.S. Surgeon General’s Advisory, www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf.

The American Psychological Association, May 2023, “Health Advisory on Social Media Use in Adolescence,” the American Psychological Association. www.apa.org/topics/social-media-internet/health-advisory-adolescent-social-media-use.

The American Psychological Association, April 2024, “Potential Risks of Content, Features, and Functions: The Science of How Social Media Affects Youth,” www.apa.org/topics/social-media-internet/youth-social-media-2024.

Twenge, J. M., Haidt, J., Lozano, J., Cummins, K. M., & Vogels, E., 2022, “Teens and Cyberbullying 2022,” Pew Research Center: Internet, Science & Tech, United States of America, www.pewresearch.org/internet/2022/12/15/teens-and-cyberbullying-2022/.

Vogels, E., Gelles-Watnick, R., & Massarat, N., 2022, “Teens, Social Media and Technology 2022,” Pew Research Center: Internet, Science & Tech, United States of America, www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/.

Weir, K., September 1, 2023, “Social Media Brings Benefits and Risks to Teens. Psychology Can Help Identify a Path Forward,” *Monitor on Psychology, American Psychological Association*, 54(6), 46, www.apa.org/monitor/2023/09/protecting-teens-on-social-media.

Social Networking Stats

Top Websites Ranking
www.similarweb.com/top-websites/games/

GLOBAL SOCIAL MEDIA STATISTICS
Favourite Social Media Platforms
Main Reasons for Using Social Media
www.datareportal.com/social-media-users

Top 32 Social Media Sites (2024)
www.explodingtopics.com/blog/top-social-media-platforms

Lyons, K., December 18, 2023, “Top 28 Social Media Platforms Worldwide,” www.semrush.com/blog/most-popular-social-media-platforms/

Social media cheat sheet — Details+Logos
This cheat sheet can help you keep track of all the different social media apps, how they might impact your child’s mental health, and what privacy and safety features are built in.
https://mhanational.org/youth-tech/social-media-cheat-sheet

Note

1 This Appendix contains references to materials provided for the reader's convenience. The inclusion of these references is not intended to reflect their importance, nor is it intended to endorse any views expressed, or products or services offered by third-party providers. These reference materials may contain the views and recommendations of various subject matter experts as well as hypertext links, contact addresses, and websites to information created and maintained by other public and private organizations.

The opinions expressed in any of these third-party materials included as references herein do not reflect the positions or policies of the authors or Publisher.

The authors do not control or guarantee the accuracy, relevance, timeliness, update, or completeness of any outside, third-party information included in this Appendix. These references should not be construed as an endorsement by the authors or the Publisher. The reader should validate and substantiate any information directly from third-party providers before acquiring, implementing, or using any product or service referenced in this Appendix.

Appendix D: Digital Badges and Certificates

Websites — Badges

The following table presents a non-exhaustive list of popular websites for creating student digital badges that educators may wish to investigate. The sites are presented alphabetically, and the URL included with each site is the most current as of November 2024.

WEBSITE NAME	DESCRIPTION	URL
Accredible	Platform for creating and distributing digital badges and certificates.	www.accredible.com
Badge designer	Tool for creating and designing digital badges.	www.badgedesigner.com
Badgecraft	Offers tools for designing and issuing open badges.	www.badgecraft.eu
BadgeOS	WordPress plugin for creating and awarding badges.	www.badgeos.org
Badgelist	Simple platform for creating and awarding digital badges.	www.badgelist.com
Badgr	Offers tools to create, manage, and share digital badges.	www.badgr.com
Badgewell	Helps educators create, manage, and share digital badges.	www.badgewell.com
BeBadges	Allows users to create and issue open badges easily.	https://oecd-opsi.org/innovations/be-badges/
Canvabadges	Integrates with Canvas LMS to award digital badges.	www.canvabadges.org
ClassBadges	Easy-to-use tool for teachers to create and award badges to students.	https://www.brighthubeducation.com/teaching-elementary-school/127670-review-of-class-badges-for-student-learning/#:~:text=The%20website%20is%20very%20easy

(*Continued*)

(***Continued***)

WEBSITE NAME	DESCRIPTION	URL
Credly	Provides a platform for issuing and managing digital credentials.	www.credly.com
ForAllRubrics	Allows educators to create, share, and track digital badges.	www.forallrubrics.com
GetBadges	Integrates with project management tools to award badges based on activities.	www.getbadges.io
Mozilla open badges	Open-source badge issuing platform.	www.openbadges.org
MyMantl	Provides a platform for creating and managing badges for learners.	https://mymantl.com/
Open badge factory	Comprehensive platform for creating and managing digital badges.	www.openbadgefactory.com
Passport by purdue	Digital badging platform developed by Purdue University.	www.purdue.edu/passport
SkillStack	Digital badging platform focused on career and technical education.	www.skillstack.idaho.gov

These websites can assist educators in issuing and managing digital badges or certificates recognizing and rewarding students for demonstrating good character skills, acceptable behavior, practicing safe cyber habits, and being good digital citizens.

Websites — Certificates

This table provides a list of popular websites with various tools and templates that educators may wish to access for assistance in creating achievement and recognition certificates for students.

WEBSITE NAME	DESCRIPTION	URL
123 certificates	Easy-to-use tool for creating printable certificates.	www.123certificates.com
Adobe spark	Provides creative tools for designing custom certificates.	www.adobe.com/express
Awardbox	Free online tool to create and print certificates.	www.awardbox.com
Canva	Offers a wide variety of customizable certificate templates.	www.canva.com
Certificate magic	Simple tool for creating and printing certificates.	www.certificatemagic.com
Certificate street	Offers a range of certificate templates for different achievements.	www.certificatestreet.com
Certificatemaker.com	Simple tool for creating custom certificates.	www.certificatemaker.com
Certify’em	Google Forms add-on for creating certificates.	www.certifyem.com

(*Continued*)

(*Continued*)

WEBSITE NAME	DESCRIPTION	URL
Free printable certificates	Large selection of free, printable certificate templates.	www.freeprintablecertificates.net
Greetings island	Customizable certificate and award templates.	www.greetingsisland.com
Jotform	Online form builder with certificate templates.	www.Jotform.com
Lucidpress	Design tool with a variety of templates, including certificates.	www.lucidpress.com
Microsoft office templates	Extensive library of certificate templates for Word and PowerPoint.	www.templates.office.com
Parchment certificates	Specializes in parchment-style certificate templates.	https://www.parchment.com/platform/higher-education/certificate-services/
PosterMyWall	Graphic design tool with certificate templates.	www.postermywall.com
SmartDraw	Diagramming tool with certificate templates.	www.smartdraw.com
Template.net	Library of professionally designed certificate templates.	www.template.net
Venngage	Infographic maker with certificate templates.	www.venngage.com
Zazzle	Customizable certificate templates for various occasions.	www.zazzle.com

Badge and Certificate — Ideas

The following table provides specific badge and certificate ideas tailored to recognize and reward students' efforts and achievements for (a) excellent academic work, (b) demonstrating good character traits/skills, (c) exhibiting acceptable behavior, (d) practicing cyber-safe habits both on- and offline, (e) speaking out against bullying, and (f) being good digital citizens.

BADGE/CERTIFICATE NAME	SUGGESTIONS FOR EDUCATORS
EXCELLENT ACADEMIC WORK	
History buff	Given to students who show excellent understanding and knowledge in history assignments.
Math whiz	Awarded for exceptional performance in math tests or assignments.
Reading rockstar	Recognizes students who achieve high scores in reading comprehension or complete multiple books.
Science superstar	Given to students who excel in science projects or experiments.
Writing champion	Awarded for outstanding essays, stories, or poetry.

(*Continued*)

(***Continued***)

BADGE/CERTIFICATE NAME	SUGGESTIONS FOR EDUCATORS
DEMONSTRATING GOOD CHARACTER TRAITS/SKILLS	
Advocate award	Recognizes students who take care of what entrusted to them.
Kindness ambassador	Recognizes students who consistently show kindness to peers and teachers.
Perseverance pro	Awarded to students who show persistence in overcoming challenges.
Respectful role model	Given to students who always show respect to others.
Responsibility hero	Recognizes students who take responsibility for their actions and schoolwork.
Teamwork titan	Awarded for excellent collaboration and teamwork in group projects.
EXHIBITING ACCEPTABLE BEHAVIOR	
Advocate champion	Awarded to students for defending the respectful behavior shown to others.
Attentiveness star	Given to students who show excellent focus and attentiveness during lessons.
Classroom leader	Given to students who demonstrate leadership qualities in the classroom.
Punctuality pro	Recognizes students who consistently arrive on time and meet deadlines.
Respectful listener	Recognizes students who listen attentively and respectfully to teachers and peers.
Rule follower	Awarded to students who consistently follow classroom and school rules.
PRACTICING CYBER-SAFE HABITS	
Cyberbullying defender	Awarded to students who take action to prevent or stop cyberbullying.
Online safety expert	Awarded for demonstrating knowledge of online safety practices.
Password protector	Given to students who understand the importance of creating and maintaining strong passwords.
Privacy guardian	Recognizes students who practice safe sharing of personal information online.
Safe surfer	Given to students who demonstrate safe browsing habits.
Sly sleuth	Awarded to students for recognizing and identifying unsafe or tricky people.
SPEAKING OUT AGAINST BULLYING	
Anti-bullying advocate	Given to students who promote anti-bullying messages and behaviors.
Bullying buster	Recognizes students who actively speak out against bullying.
Inclusive ally	Awarded to students who make efforts to include everyone and prevent exclusion.
Peacekeeper	Recognizes students who help resolve conflicts among peers.
Upstander award	Awarded to students who support peers being bullied and stand up for them.
BEING GOOD DIGITAL CITIZENS	
Digital etiquette expert	Recognizes students who show good manners and respect in digital communications.
Ethical user	Awarded for demonstrating ethical behavior in online activities.
Informed netizen	Recognizes students who stay informed about digital citizenship topics.
Positive poster	Given to students who contribute positively to online discussions and social media.
Responsible digital citizen	Given to students who understand and practice responsible digital citizenship.

Digital Badge — Conceptual Designs

This table provides conceptual design ideas to help educators visualize, sketch, and create the digital badges previously identified.

BADGE/CERTIFICATE NAME	DESCRIPTION OF BADGE APPEARANCE
EXCELLENT ACADEMIC WORK	
History buff	A historical building (like a temple or ancient structure) with a laurel wreath on a brown background.
Math whiz	A badge featuring a calculator and math symbols (plus, minus, multiplication, division) on a blue background.
Reading rockstar	An open book with a shining star above it on a purple background.
Science superstar	A star-shaped badge with a microscope and a test tube with colorful liquid on a green background.
Writing champion	A quill pen writing on a parchment scroll with a gold medal ribbon on a white background.
DEMONSTRATING GOOD CHARACTER TRAITS/SKILLS	
Advocate champion	A badge featuring a shield with a heart in the center, symbolizing protection and care. Two hands, one on each side of the shield, are shown raised in a gesture of support and defense. The background is a blend of warm colors like orange and gold, indicating the positive impact and strength of advocacy for respectful behavior.
Kindness ambassador	A heart-shaped badge with hands holding it gently on a pink background.
Perseverance pro	A mountain with a flag on top, symbolizing achievement, on an orange background.
Respectful role model	A badge with a person bowing or showing respect, framed by a circle on a green background.
Responsibility hero	A superhero cape with a checkmark emblem on a red background.
Teamwork titan	Interlocking hands or puzzle pieces forming a team symbol on a yellow background.
EXHIBITING ACCEPTABLE BEHAVIOR	
Advocate award	A badge featuring a pair of caring hands gently holding a treasure chest, symbolizing the responsibility and care for entrusted items. The treasure chest is slightly open, showing a glowing light, indicating the value and importance of what is being protected. The background is a gradient of green and gold, representing growth and value.
Attentiveness star	An eye symbol with a sparkle, indicating attentiveness, on a yellow background.
Classroom leader	A badge with a podium and a student speaking or leading a group, on a blue background.
Punctuality pro	A clock with a checkmark and rays of light to indicate promptness, on a light blue background.
Respectful listener	A pair of ears with sound waves, indicating active listening, on a light green background.
Rule follower	A rule book with a checkmark on a dark green background.
PRACTICING CYBER-SAFE HABITS	
Cyberbullying defender	A badge with a crossed-out speech bubble containing negative words, on a red background.
Online safety expert	A shield with a lock symbol on a blue background.
Password protector	A key with a shield emblem, symbolizing secure passwords, on a light blue background.
Privacy guardian	A privacy symbol with a shield and an eye with a line through it, on a gray background.
Safe surfer	A surfboard on a wave with a lock symbol, indicating safe browsing, on a light green background.
Sly sleuth	A badge featuring a magnifying glass over a shadowy figure, symbolizing careful observation and detection. The magnifying glass is held by a detective hat-wearing character, representing a clever sleuth. The background is a dark blue, with subtle rays of light emanating from the magnifying glass to highlight the idea of uncovering the truth.

(*Continued*)

(***Continued***)

BADGE/CERTIFICATE NAME	DESCRIPTION OF BADGE APPEARANCE
SPEAKING OUT AGAINST BULLYING	
Anti-bullying advocate	A megaphone with a no-bullying symbol, indicating advocacy, on a light blue background.
Bullying buster	A superhero figure with a crossed-out bullying sign on their chest, on a red background.
Inclusive ally	A group of diverse figures holding hands, indicating inclusion, on a rainbow background.
Peacekeeper	A dove holding an olive branch, symbolizing peacekeeping, on a white background.
Upstander award	A person standing tall with hands raised, representing standing up for others, on a yellow background.
BEING GOOD DIGITAL CITIZENS	
Digital etiquette expert	A computer screen with a handshake symbolizing good manners online, on a blue background.
Ethical user	A scale symbol representing ethics, on a gold background.
Informed netizen	A computer screen with a light bulb, symbolizing being informed, on a light blue background.
Positive poster	A speech bubble with a thumbs-up symbol, indicating positive online contributions, on a purple background.
Responsible digital citizen	A globe with a checkmark, indicating global digital responsibility, on a green background.

Appendix E: AI Frameworks

Why Choose an Artificial Intelligence Framework?

An artificial intelligence (AI) framework is a comprehensive software platform designed to simplify the development of AI models. It provides a structured environment with pre-built components and tools for designing, training, evaluating, and deploying machine learning and deep learning models.

AI libraries are collections of pre-written code that provide specific functionalities or algorithms for AI development. They are often used within frameworks but can also be used independently.

How AI Frameworks and Libraries Benefit Users

1. Accelerate Development: By providing pre-built components and tools, frameworks and libraries help developers build and iterate on models more quickly.
2. Reduce Complexity: They abstract complex mathematical and computational operations, making it easier for users to focus on higher-level tasks and problem-solving.
3. Improve Accuracy: Frameworks and libraries often come with state-of-the-art algorithms and pretrained models that can improve the accuracy and performance of AI applications.
4. Promote Collaboration: Many frameworks and libraries are open-source, fostering collaboration and knowledge sharing among researchers and developers.
5. Support Diverse Applications: They cater to various types of AI tasks, including computer vision, natural language processing, and reinforcement learning, enabling users to tackle a wide range of problems.

AI frameworks and libraries are essential tools that streamline the AI development process, enhance model performance, and make sophisticated AI techniques more accessible to users with varying levels of expertise.

The following table provides a summary of AI framework and guidance, as of November 2024, that educators may decide to investigate and use to further enhance the classroom discussion on AI, and AI literacy.

EXISTING FRAMEWORKS AND GUIDANCE FOR AI AND AI IN EDUCATION

K—12 EDUCATION

RESOURCE	SUMMARY
AI guidance for schools toolkit Teach AI, www.teachai.org/toolkit	The AI Guidance for Schools Toolkit is designed to help local, state, and national education systems worldwide develop guidance on the responsible use of AI, ensure compliance with relevant policies, and build the capacity of all stakeholders to understand AI and use AI effectively. The toolkit contains six principles for AI in education: 1. Knowledge: Promote AI literacy 2. Integrity: Advance academic integrity 3. Evaluation: Regularly assess the impacts of AI 4. Compliance: Reaffirm adherence to existing policies 5. Balance: Realize the benefits of AI and address the risks 6. Agency: Maintain human decision-making when using AI.
K—12 AI guidelines AI4K12, https://ai4k12.org/	AI4K12 is developing national guidelines for AI education for K—12, as well as instructional resources and a community of practitioners. The guidelines contain five big ideas: 1. Perception 2. Representation & Reasoning 3. Learning 4. Natural Interaction 5. Societal Impact.
AI in education toolkit for racial equity The EdTech Equity Project, https://coda.io/@edtechequity/edtech-ai-toolkit-for-racial-equity	The AI in Education Toolkit for Racial Equity aims to mitigate bias in the design and development of edtech products and tools. The toolkit contains eight phases of design within which critical questions related to racial equity are explored: 1. Ideation 2. Logical Assumptions 3. Content 4. Datasets 5. Training Algorithms 6. UX Design 7. Testing & Evaluation 8. Implementation.

(*Continued*)

(*Continued*)

EXISTING FRAMEWORKS AND GUIDANCE FOR AI AND AI IN EDUCATION

K—12 EDUCATION

RESOURCE	SUMMARY
Artificial intelligence and the future of teaching and learning U.S. Department of Education, Office of EdTech, www2.ed.gov/documents/ai-report/ai-report.pdf	The Office of EdTech outlined a set of recommendations to engage teachers, educational leaders, policymakers, researchers, educational technology innovators, and providers, as they work toward policy action related to AI in education. 1. Emphasize Humans-in-the-Loop 2. Align AI Models to a Shared Vision for Education 3. Design AI Using Modern Learning Principles 4. Prioritize Strengthening Trust 5. Inform and Involve Educators 6. Focus R&D on Addressing Context and Enhancing Trust and Safety 7. Develop Education-specific Guidelines and Guardrails.
The ethical framework for AI in education the institute for ethical AI in education, www.buckingham.ac.uk/wp-content/uploads/2021/03/The-Institute-for-Ethical-AI-in-Education-The-Ethical-Framework-for-AI-in-Education.pdf	The Framework is grounded in a shared vision of ethical AI in education and will help to enable all learners to benefit optimally from AI in education, whilst also being protected against the risks this technology presents. These principles include impacting: 1. Achieving Educational Goals 2. Forms of Assessment 3. Administration & Workload 4. Equity 5. Autonomy 6. Privacy 7. Transparency & Accountability 8. Informed Participation 9. Ethical Design.
K—12 Computer Science content standards Computer Science Teachers Association (CSTA), https://csteachers.org/k12standards/interactive/	The CSTA K—12 Computer Science Standards delineate a core set of learning objectives designed to provide the foundation for a complete computer science curriculum and its implementation at the K—12 level. The five core concepts of the standards are as follows: 1. Computing Systems 2. Networks and the Internet 3. Data and Analysis 4. Algorithms and Programming 5. Impacts of Computing.
K—12 CS teacher standards Computer Science Teachers Association (CSTA), https://csteachers.org/teacherstandards/interactive/	The Standards for CS Teachers establish robust standards to help teachers deliver effective and equitable CS instruction in support of rigorous CS education for all K—12 students. There are five standards: 1. CS knowledge and skills 2. Equity and Inclusion 3. Professional Growth and Identity 4. Instructional Design 5. Classroom Practice.

(*Continued*)

(***Continued***)

EXISTING FRAMEWORKS AND GUIDANCE FOR AI AND AI IN EDUCATION

K—12 EDUCATION

RESOURCE	SUMMARY
Advanced Placement CS principles College Board, https://apcentral.collegeboard.org/media/pdf/ap-computer-science-principles-course-and-exam-description.pdf	AP Computer Science Principles introduces students to the breadth of the field of computer science, learning to design and evaluate solutions, solve problems through the development of algorithms and programs, explain how computing innovations and computing systems, including the Internet, work, explore their potential impacts, and contribute to a computing culture that is collaborative and ethical. AP CS P contains five big ideas: 1. Creative Development 2. Data 3. Algorithms & Programming 4. Computing Systems & Networks 5. Impacts of Computing.
AP CS A College Board, https://apcentral.collegeboard.org/media/pdf/ap-computer-science-a-course-and-exam-description.pdf	AP Computer Science A introduces students to computer science through programming, with topics including the design of solutions to problems, the use of data structures to organize large sets of data, the development and implementation of algorithms to process data and discover new information, the analysis of potential solutions, and the ethical and social implications of computing systems. AP CS A contains four big ideas: 1. Modularity 2. Variables 3. Control 4. Impact of Computing.
SAFE benchmarks framework EDSAFE AI Industry Council, www.edsafeai.org/safe	The Framework creates a policy process and roadmap for the essential issues in creating a SAFE AI ecosystem. EDSAFE aims to accomplish two things: achieve equitable outcomes for students and improve working conditions for teachers. The framework consists of four major categories: 1. Safety 2. Accountability 3. Fairness and Transparency 4. Efficacy.
AI literacy framework Kennedy HQ, https://kennedyhq.com/wp/2023/12/21/ai-literacy-framework/?trk=public_post_comment-text	The AI Literacy Framework's foundation is the UNESCO Digital Literacy Global Framework to which AI skills are mapped. The framework consists of seven categories: 1. Hardware & Software 2. Information & Data Literacy 3. Communication & Collaboration 4. Content Creation 5. Safety 6. Problem-solving 7. Career Competencies.

(*Continued*)

(*Continued*)

EXISTING FRAMEWORKS AND GUIDANCE FOR AI AND AI IN EDUCATION

K—12 EDUCATION

RESOURCE	SUMMARY
The 4As: Ask, Adapt, Author, Analyze — AI literacy framework for families MIT Press Works in Progress (WiP), https://wip.mitpress.mit.edu/pub/the-4as/release/1	With the objective to ensure algorithmic fairness, this framework can be used by families for developing a critical understanding of smart technologies embedded in their lives. The 4As AI literacy framework is composed of four main dimensions (4As): 1. Ask 2. Adapt 3. Author 4. Analyze.
AI literacy framework Digital Promise, https://digitalpromise.org/2024/02/21/revealing-an-ai-literacy-framework-for-learners-and-educators/	A comprehensive Framework for AI Literacy that seeks to empower district leaders, teachers, and learners to make informed decisions about how to integrate AI in the world and specifically in education. The framework emphasizes that understanding and evaluating AI are critical to making informed decisions about if and how to use AI in learning environments. The AI Literacy Framework includes three components: 1. Understand 2. Use 3. Evaluate.

AI & TECH POLICY

RESOURCE	SUMMARY
AI bill of rights The White House Office of Science and Technology Policy, https://bidenwhitehouse.archives.gov/ostp/ai-bill-of-rights/	The AI Bill of Rights outlines five principles that should guide the design, use, and deployment of automated systems that are aligned with democratic values and protect civil rights, civil liberties, and privacy. This framework applies to (a) automated systems that (b) have the potential to meaningfully impact the American public's rights, opportunities, or access to critical resources or services. 1. Safe and Effective Systems 2. Algorithmic Discrimination Protections 3. Data Privacy 4. Notice and Explanation 5. Human Alternative, Consideration and Fallback.
Advancing racial equity through tech policy AI Now, https://ainowinstitute.org/publication/advancing-racial-equity-through-technology-policy	This resource argues for centering racial equity in the technology policy debate and outlines a five-point policy agenda for doing so: 1. Center racial equity in tech regulatory efforts 2. Promote democratic governance of technology 3. Build an equitable tech labor market 4. Ensure equitable access to goods, services, and information 5. Eliminate disparities in tech ownership and entrepreneurship.

(*Continued*)

AI & TECH POLICY

RESOURCE	SUMMARY
Confronting tech power AI Now, https://ainowinstitute.org/general/2023-landscape-executive-summary	This report aims to provide strategic guidance on the many levers we can use to shape the future trajectory of AI — and the tech industry behind it — to ensure that it is the public, not industry, that this technology serves — in the following areas: 1. Contain tech firm's data advantage 2. Build support for competition reforms as a key lever to reduce, concentration in tech 3. Regulate ChatGPT and other large-scale models 4. Displace audits as the primary policy response to harmful AI 5. Future proof against the quiet expansion of biometric surveillance into new domains 6. Enact strong curbs on worker surveillance 7. Prevent "international preemption" by digital trade agreements which can be used to weaken national regulation on algorithmic accountability and competition policy.
RAI toolkit Responsible AI-Department of Defense, https://rai.tradewindai.com/	The Responsible Artificial Intelligence (RAI) Toolkit provides a centralized process that identifies, tracks, and improves the alignment of AI projects to RAI best practices and the DoD AI Ethical Principles while capitalizing on opportunities for innovation. The RAI Toolkit provides an intuitive flow guiding the user through tailorable and modular assessments, tools, and artifacts throughout the AI product lifecycle. The process enables traceability and assurance of responsible AI practice, development, and use.

White, S., Scott, A., & Koshy, S., January 18, 2024, "Responsible AI & Tech Justice: A Guide for K-12 Education, – Appendix 3," Kapor Foundation, https://kaporfoundation.org/wp-content/uploads/2024/01/Responsible-AI-Guide-Kapor-Foundation.pdf, used with permission as provided through CC BY-ND 4.0, Attribution-NoDerivatives 4.0 International, Creative Commons License, http://creativecommons.org/licenses/by-nd/4.0/, Authors added individual resource site URLs, the S.A.F.E. Benchmarks Framework, the AI Literacy Framework, The 4As: AI Literacy Framework for Families, The AI Literacy Framework, to original appendix content, retrieved August 20, 2024.

Readers interested in further information and a review of additional AI frameworks beyond those identified above are directed to the following resource…

Melnik, Y., September 2023, "The Top 16 AI Frameworks and Libraries: A Beginner's Guide," Datacamp, www.datacamp.com/blog/top-ai-frameworks-and-libraries.

Appendix F: Hidden Dangers

Identifying Risky Apps on Your Child's Device

Addressing Cyber Safety through an App Review

The concern with both general and specific social media and social networking risks and a child's access to potentially dangerous content warrants the performance of a periodic App Review.

An App Review is straightforward and nontechnical. The objectives are to (a) take a proactive role in keeping your child safe, (b) identify potentially inappropriate or even dangerous apps that may be installed on your child's phone (either intentionally installed or installed automatically due to the user's activities and sites visited), and (c) effectively uninstall apps which could potentially place your child (and potentially their family and friends) at risk.

Inappropriate Apps for Seventh- and Eighth-Grade Students

Examples of apps that may be considered inappropriate, if found installed on a tween's phone, would be the following:

- Snapchat
  - Why Would This App Be Considered Inappropriate?
    - Snapchat allows users to send disappearing messages, which can encourage risky behavior like sharing personal information, inappropriate images, or messages. While it may seem harmless, the platform's features like "Snap Map," which shares the user's location, and the potential for exposure to inappropriate content through the "Discover" section, make it a questionable choice for tweens.

OmeTV (or other anonymous chat apps)

Why Would This App Be Considered Inappropriate?

OmeTV is a live video chat app that allows users to connect with and engage in unsupervised interaction with strangers. Tweens may use it out of curiosity or for fun. Still, it's notorious for exposing young users to inappropriate content, predatory behavior, and interactions with strangers who may have malicious intentions. The lack of supervision, accountability, and anonymity make it highly unsafe for young users.

Apps Considered Dangerous for Seventh- and Eighth-Grade Students

Examples of apps that may be considered dangerous, if found installed on a tween's phone, would be the following:

Kik Messenger (Kik)

Why Would This App Be Considered Dangerous?

Kik allows users to chat with strangers anonymously, which can lead to dangerous interactions with unverified individuals, including potential predators. It lacks strong parental controls, making it difficult for parents to monitor their children's conversations and online activity. Additionally, the platform has been associated with the sharing of explicit content, which can easily expose young users to inappropriate material, cyberbullying, and child grooming. Kik is listed as 17+ in app stores, but the app targets teens: around 70% of the app's users are between the ages of 13 and 24.[1]

TikTok (Unmonitored)

Why Would This App Be Considered Dangerous?

TikTok exposes tweens to a wide range of content, including explicit language, suggestive dances, and potentially dangerous challenges, making it hard to control what they view. Without strict privacy settings, young users can interact with strangers through comments or direct messages, increasing the risk of unwanted or inappropriate interactions. The app's design encourages endless scrolling, which can lead to excessive screen time and negative impacts on mental health.[2]

Performing an App Review of a Mobile Device

The following stepwise procedures are provided to assist parents, trusted adults, caregivers, and if and when appropriate, educators in identifying potentially inappropriate and/or dangerous apps on mobile phones.

Steps to identify apps on an Apple iPhone are presented first, followed by steps for Android devices.

Apple iPhone

Step 1: Check for Hidden Apps in Folders

Sometimes, apps are hidden in folders to make them less noticeable. Here's how to check:

1. Go to the **Home Screen**.
2. Swipe through all the Home screens and look inside every folder.
3. Long-press on each folder to see its name and contents. Hidden apps might be in deep subfolders, so check multiple levels.

Step 2: Use Spotlight Search

Even if an app is hidden, it can still appear in search results unless specifically restricted.

1. From the Home Screen, **swipe down** to bring up the search bar (Spotlight Search).
2. Type the name of the suspected app.
3. If the app appears in the search results, it is installed on the device.

Step 3: Review App Store Purchase History

If apps have been hidden or deleted from the Home screen, they might still be listed in the App Store's purchase history.

1. Open the App Store.
2. Tap on your profile picture in the upper-right corner.
3. Select Purchased.
4. Review the list of apps. If you see an app with a cloud icon, it means it has been downloaded before but is not currently installed.

Step 4: Check Screen Time for Hidden Apps

Screen Time is a useful feature for managing app usage. Here's how to see all the apps being used:

1. Open Settings and tap Screen Time.
2. Tap See All Activity to get a detailed breakdown of app usage.
3. Review apps listed under Most Used. Hidden apps may still show up here if they have been used recently.

Step 5: Review Installed Apps List

Another method to see all installed apps is by viewing the storage information:

1. Go to Settings → General → iPhone Storage.
2. Wait for the list of apps to populate. This will show all apps installed on the device, including hidden ones.
3. Scroll through and see if there are any apps that seem suspicious or unfamiliar.

Step 6: Check for Virtual Private Networks (VPN) or App Lockers

Tweens might use VPNs or special app lockers to hide apps or mask their activity.

1. Go to **Settings** → **General** → **VPN**. If there's an active VPN connection, this could indicate they are hiding activity.
2. Look for apps like "Vault" or "Calculator+," which are designed to hide apps or photos.

Step 7: Disable App Restrictions

If the tween has used restrictions to hide apps, you can temporarily disable this feature:

1. Open Settings → Screen Time → Content & Privacy Restrictions.
2. Tap iTunes & App Store Purchases → Installing Apps and ensure it is set to Allow.
3. Disable App Limits and Downtime if they have been enabled to reduce app visibility.

Step 8: Check for Hidden Apps in the App Library

The App Library organizes all apps on the device, even those not visible on the Home Screen.

1. Go to the **App Library** by swiping left until you reach the end of the Home Screen.
2. Review all the app categories and look for hidden or unfamiliar apps.
3. If you spot an app that's not on the Home Screen, it might be hidden.

Step 9: Identify Suspicious Apps

If you find any unfamiliar apps, research them online to see if they are designed for deception (e.g., Vault apps or apps for hiding content).

Step 10: Uninstall Hidden or Suspicious Apps

Once you identify an app you want to remove, here's how to uninstall it:

1. Go to the Home Screen or the App Library.
2. Press and hold the app icon until a menu appears.
3. Select Remove App.
4. Confirm by tapping Delete App.

Alternatively, you can also delete apps through the iPhone Storage list:

1. Go to Settings → General → iPhone Storage.
2. Select the app you want to remove.
3. Tap Delete App.

Android Phone

Step 1: Check the App Drawer[3] for Hidden Apps

Some tweens may hide apps by disabling the visibility in the app drawer.

1. Open the **App Drawer** by swiping up from the Home screen.
2. Look through the list of apps and check for any unfamiliar or suspicious ones.
3. Tap on the three dots or **menu icon** in the top-right corner (this may vary based on the Android version), then select **Show Hidden Apps** or **Hide Apps** to reveal any apps that have been concealed.

Step 2: Search for Apps Using Google Search or App Search

Even if an app is hidden from the app drawer, it can still be searched for.

1. Open the search bar at the top of the Home screen (Google search bar) or swipe down to open the **App Search** function.
2. Type the name of the app you suspect is hidden (e.g., social media, vault, or messaging apps like "Snapchat" or "Vault").
3. If the app is installed, it will appear in the search results.

Step 3: Check for Recently Installed Apps in the Play Store

You can review recently installed apps through the Play Store's history.

1. Open the **Google Play Store** app.
2. Tap on your **profile icon** in the upper-right corner.
3. Select **Manage apps & device → Manage**.
4. From the dropdown menu, choose **Installed** and then sort by **Recent** to view apps that have been installed recently. Look for unfamiliar or hidden apps.

Step 4: Review App Permissions

Suspicious apps may try to access sensitive information through their permissions.

1. Go to **Settings → Apps & Notifications → App Permissions**.
2. Check categories like **Camera**, **Location**, **Storage**, and **Contacts**.
3. Review which apps have permission to access these features, as vault or hidden apps may need camera or storage access. If something looks suspicious, investigate further.

Step 5: Review Storage Usage

Some hidden apps may still take up storage space, so you can check the list of installed apps by storage usage.

1. Open **Settings → Storage → Internal Storage**.
2. Tap on **Apps** to see all installed apps listed by the space they take up. Even hidden apps will show up here.
3. Look for apps that use significant storage space but don't appear in the app drawer.

Step 6: Disable Device Administrator Access

Certain apps, especially vault apps, may have device administrator privileges, which could make them harder to uninstall.

1. Go to **Settings → Security → Device Administrators**.
2. Review the list of apps that have administrative access.
3. If an unfamiliar app has administrator access, disable it by tapping the switch next to its name.

Step 7: Check for Hidden Apps Using Third-Party Apps or Developer Options

If you're still unsure whether apps are hidden, you can enable developer options or use third-party apps designed to detect hidden apps.

1. To enable **Developer Options**, go to **Settings → About Phone →** tap **Build Number** seven times to unlock Developer Mode.
2. In **Developer Options**, look under **Running Services** or **Processes** to see if any apps are running that don't appear in the app drawer.

Step 8: Check for App Lockers or Vault Apps

Tweens may use specific apps designed to hide or lock content, like vault apps or app lockers.

1. Search for terms like "Vault," "App Lock," "Secret," or "Calculator+" (some vault apps disguise themselves as calculators).
2. Check app permissions, as vault apps often need access to photos, videos, or other sensitive information.

Step 9: Review Apps Installed Using APK Files

Some tweens may bypass the Play Store by installing APK files, which won't show up in the usual app listings.

1. Go to **Settings → Apps & Notifications → Special App Access → Install Unknown Apps**.
2. Review which apps have permission to install unknown apps (e.g., browsers, file managers).
3. Check for recently downloaded APKs or apps installed through third-party sources.

Step 10: Uninstall Suspicious or Hidden Apps

Once you identify an app you want to remove, follow these steps to uninstall it:

1. Go to **Settings → Apps & Notifications → See All Apps**.
2. Find the app in the list, tap on it, and select **Uninstall**.
3. If the app is a device administrator, go back to **Security → Device Administrators** and remove its privileges first, then uninstall it.

Alternatively, you can uninstall apps directly from the app drawer by

1. long-pressing the app icon and
2. selecting **Uninstall** from the options that appear.

Summary

By following the above steps, iPhones and Android devices can be methodically reviewed to uncover hidden apps individuals may be using on their mobile devices.

Notes

1 Woodward, M., June 23, 2024, "Kik 2024 User Statistics: How Many People Use Kik?" Search Logistics, www.searchlogistics.com/learn/statistics/kik-user-statistics/#:~:text=Kik's%20biggest%20and%20most%20active,active%20users%20on%20the%20app, retrieved September 12, 2024.

2 JRRJ Blog, December 7, 2022, "Is TikTok Safe for Children?" *Journal of Gender, Race & Justice (JGRJ)*, Iowa University, jgrj@uiowa.edu, https://jgrj.law.uiowa.edu/news/2023/01/tiktok-safe-children, retrieved September 12, 2024.

3 App drawer is a feature found in mobile device operating systems such as Android. It is a menu that shows all the apps installed on your device. On most Android devices, you can access the app rawer by tapping on the "apps" icon located on your home screen.

Appendix G: The Anatomy of Cybersecurity Attacks in the Consumer Space

Written by Mathias Conradt

Introduction

This appendix discusses the anatomy of targeted cyberattacks against consumers, particularly focusing on their methods and techniques to highlight how individuals can better protect themselves.

Cyberattacks against consumers, especially children and teenagers, differ from those against business personas due to their distinct vulnerabilities. A targeted cyberattack typically involves gathering information, crafting a convincing attack, and exploiting the obtained data for various malicious purposes.

A fictitious example of a cyber attacker targeting video game players is used to illustrate how attackers lure victims with fake offers. This tactic has real-world parallels, such as the case of fake Nintendo websites in 2022.

Information Gathering

The Cyber Attacker's Approach

A cyber attacker begins their preparation for an attack by utilizing open-source intelligence (OSINT) techniques to identify potential victims. Their focus is often on young adults who are active gamers, particularly those who play on popular platforms like Nintendo Switch, PlayStation, Microsoft Xbox, Steam, and others.

To find these individuals, the attacker combs through social media profiles, using platforms like Twitter, Instagram, or TikTok. They search for specific terms such as

"PlayStation," "Nintendo," or the names of well-known games, narrowing down their target audience.

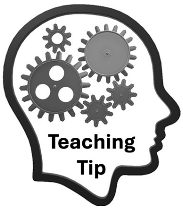
The attacker is particularly interested in a demographic that is old enough to have personal email addresses and their own smartphones, yet still young and potentially inexperienced with online security. This group, which may include tweens and teens, is often more trusting and less likely to recognize the signs of a scam, making them ideal targets. While many social media platforms set their age requirements at 13, the attacker is aware that even younger children might create accounts, further broadening the pool of potential victims.

From the information found on these social media accounts, the attacker gathers crucial details such as the victim's username or player handle on gaming platforms, the names or gaming handles of their friends, and their favorite games and characters. This data allows the attacker to build a detailed profile of the victim, which they will later exploit.

With this information, the attacker crafts a highly personalized message designed specifically for the victim. This message is carefully tailored, incorporating references to the victim's gaming preferences, friends, and online activities, making it appear legitimate and trustworthy. The goal is to make it difficult for the victim to realize that the message is a carefully orchestrated attempt to deceive them and gain access to their personal information or accounts.

How to Protect Yourself against Becoming a Victim?

The following proactive learning objectives should be shared with students. Such actions will assist students to avoid falling victim to this type of cyber risk.



Educators should aim to teach students:

- How to practice safe social media habits by avoiding oversharing personal information and ensuring privacy settings are configured to protect against unwanted access.
- How to identify and avoid fake friend requests from cyber attackers on social media and gaming platforms, such as TikTok, Instagram, PlayStation Network, and Nintendo Switch.
- The importance of understanding digital footprints, emphasizing that even deleted online posts may remain archived through tools like the Wayback Machine.
- To Google themselves to uncover old, forgotten content and recognize the lasting impact of what they post online.
- How to delete unwanted personal data from online accounts and recommend tools like "Just Delete Me" or paid services like DeleteMe for more comprehensive removal.
- The significance of data breaches and how private information, even if shared cautiously, can still be exposed through attacks on online services.

- How to use data breach databases and notification services, such as Breachsense and HaveIBeenPwned, to monitor for leaked information and take precautionary steps like changing compromised passwords.
- The value of subscribing to breach notification services and reviewing breach details through platforms like HaveIBeenPwned or ScatteredSecrets to ensure their online security.

Safe Social Media Practices

Avoid Oversharing

When sharing personal information online, such as your real name, date of birth, or personal posts, it's important to limit this visibility to friends, family, and those you genuinely trust. To protect your privacy, set your sharing preferences to "private" rather than "public." Most social media platforms allow you to adjust your default sharing settings, and it's wise to ensure these are configured to protect your information from being accessible to strangers.

Be cautious of friend requests from people you don't know personally. Cyber attackers often use fake profiles to send friend requests, hoping to gain access to private posts that aren't publicly visible. Only accept friend requests if you can verify the identity of the person on the other side.

These tactics can occur on social media platforms like TikTok, Instagram, and Twitter, as well as on gaming console companion platforms such as PlayStation's PSN (PlayStation Network) or Nintendo Switch. While the gaming scenario is used as an example here, these practices apply across various online contexts. Staying vigilant and maintaining strict privacy settings can significantly reduce your risk of falling victim to such attacks.

Understanding Digital Footprints

Wayback Machine (Internet Archive)

Whatever you post online, even if you delete it later, may remain on the Internet in caches or archives. For example, the Wayback Machine, also known as the Internet Archive, available at https://web.archive.org, has archived hundreds of billions of web pages over time, with some dating back to the 1990s. By entering a URL, users can view snapshots of websites from different points in history.

The reader may be interested in checking out the following URL: https://web.archive.org/web/19961220155557/http://www.aol.com/, for example. Following this link, you will see the AOL (America Online) website as it was in 1996.

However, while the Internet Archive is vast, it doesn't capture the entire web. For instance, it doesn't archive X (formerly Twitter) for some reason. Additionally, websites that require a login to view content, like LinkedIn profiles, are generally not archived by the Wayback Machine.

Google Yourself

Googling yourself can be quite interesting.

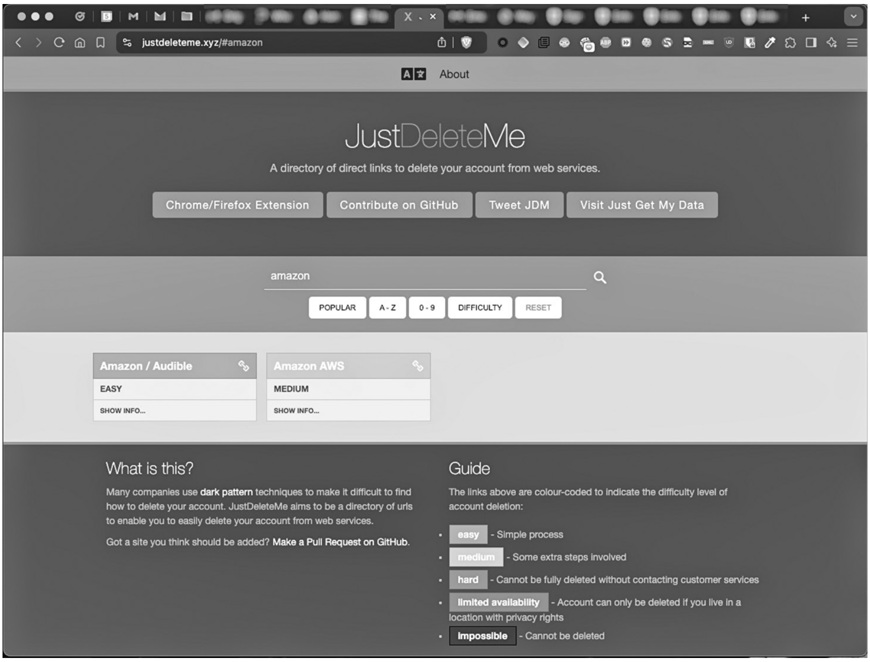
Simply type your name into the Google search engine and see what comes up—you might be surprised. You may find old content, forum posts, or social media comments that you have forgotten about and might prefer weren't public anymore. Keep in mind that everything posted online, especially in public forums, can leave a lasting digital footprint.

Deleting Unwanted Data

While it is not always possible to delete personal data from the Internet, in certain cases it can be done.

Online services, online forums, or social media platforms that hold your personal information usually allow you to delete your user account or information in it. So, as long as you have access to that account, it should be easy to delete personal information or even close an account that is not in use anymore.

There are websites out there that help with finding the right steps to delete an account, such as the website Just Delete Me[1] for example (see Figure G.1), which lists hundreds of online services and their way to get an account removed. You will still need to execute the mentioned steps to do the account closing, but the link collection helps to find these steps easily.



justdeleteme.xyz/#amazon
About
JustDeleteMe
Chrome/Firefox Extension
Contribute on GitHub
Tweet JDM
Visit Just Get My Data
amazon
POPULAR
A - Z
0 - 9
DIFFICULTY
RESET
Amazon / Audible
EASY
SHOW INFO...
Amazon AWS
MEDIUM
SHOW INFO...

A directory of direct links to delete your account from web services.

What is this?

Many companies use **dark pattern** techniques to make it difficult to find how to delete your account. JustDeleteMe aims to be a directory of urls to enable you to easily delete your account from web services.

Got a site you think should be added? **Make a Pull Request on GitHub.**

Guide

The links above are colour-coded to indicate the difficulty level of account deletion:

- **easy** - Simple process
- **medium** - Some extra steps involved
- **hard** - Cannot be fully deleted without contacting customer services
- **limited availability** - Account can only be deleted if you live in a location with privacy rights
- **impossible** - Cannot be deleted

Figure G.1 JustDeleteMe website.[2]

Other approaches are to use paid services such as **Incogni**[3] or **DeleteMe**,[4] where you submit your personal information for removal from search engines and data broker sites. DeleteMe experts then find and remove your personal information, while you receive a detailed report of the progress some days later. These services then remove your personal information regularly, all year long, while you would pay a subscription fee.

Often proactive corporate cybersecurity teams work with services like DeleteMe because they have experienced firsthand how employee and executive personally identifiable information is used in successful cyberattacks. The same applies to the consumer segment as well of course.

Understanding the Importance of Data Breaches

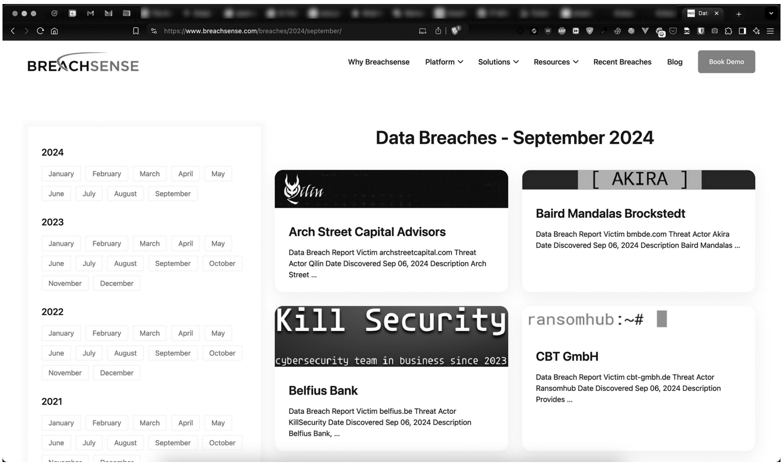
Even if you're very cautious about how you browse the Internet and what information you share publicly, your private data—such as personal account details from online services, including your order history and payment information—could still be exposed through data breaches. These breaches are often carried out by cyber attackers targeting the online service itself, rather than individual users.

Data Breach Databases and Notification Services

Services like Breachsense[5] (see Figure G.2) and HaveIBeenPwned[6] (see Figure G.3) monitor and index the dark web for leaked credentials, session tokens, company data, and potential upcoming attacks. They can send you alerts if any of your data is found in a breach, allowing you to mitigate the risk before it's exploited.

These services also display recent breaches on their websites, giving you insight into which companies have been attacked and the volume of data exposed. Often, this data includes personal information like usernames, full names, email addresses, and sometimes even passwords or hashed passwords.

If you use one of these services, it's worth reviewing the details and taking precautionary steps, such as changing your passwords on affected platforms.


https://www.breachsense.com/breaches/2024/september/
BREACHSENSE
Why Breachsense
Platform
Solutions
Resources
Recent Breaches
Blog
Book Demo
2024
January February March April May
June July August September
2023
January February March April May
June July August September October
November December
2022
January February March April May
June July August September October
November December
2021
January February March April May
June July August September October
Qilin
[AKIRA]
Kill Security
cybersecurity team in business since 2023
ransomhub:~#

Data Breaches - September 2024

Arch Street Capital Advisors

Data Breach Report Victim archstreetcapital.com Threat Actor Qilin Date Discovered Sep 06, 2024 Description Arch Street ...

Baird Mandalas Brockstedt

Data Breach Report Victim bmbde.com Threat Actor Akira Date Discovered Sep 06, 2024 Description Baird Mandalas ...

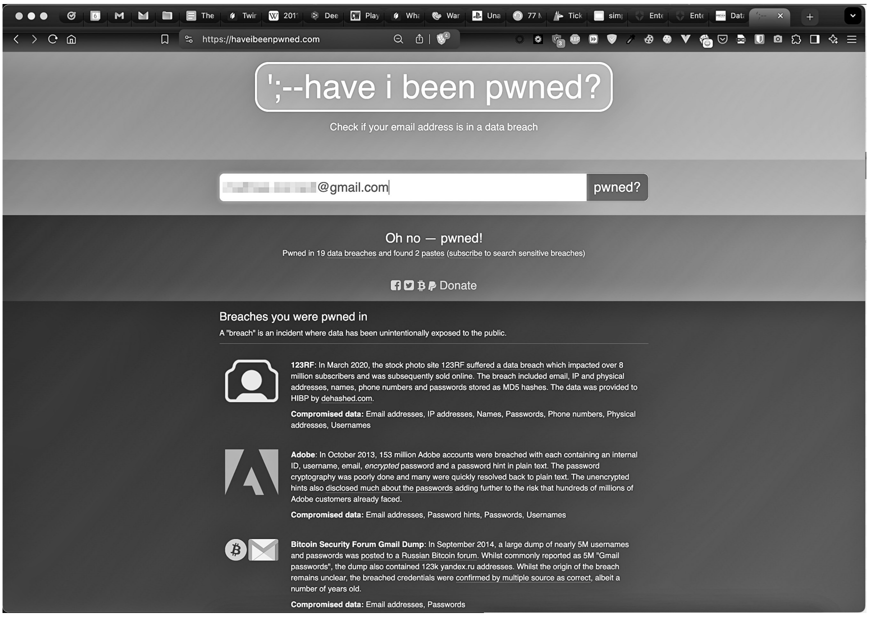
Belfius Bank

Data Breach Report Victim belfius.be Threat Actor KillSecurity Date Discovered Sep 06, 2024 Description Belfius Bank, ...

CBT GmbH

Data Breach Report Victim cbt-gmbh.de Threat Actor Ransomhub Date Discovered Sep 06, 2024 Description Provides ...

Figure G.2 Breachsense — data breaches, September 2024.[7]


https://haveibeenpwned.com
';--have i been pwned?
pwned?
Donate

Check if your email address is in a data breach

[redacted]@gmail.com

Oh no — pwned!

Pwned in 19 data breaches and found 2 pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where data has been unintentionally exposed to the public.

123RF: In March 2020, the stock photo site 123RF suffered a data breach which impacted over 8 million subscribers and was subsequently sold online. The breach included email, IP and physical addresses, names, phone numbers and passwords stored as MD5 hashes. The data was provided to HIBP by dehashed.com.

Compromised data: Email addresses, IP addresses, Names, Passwords, Phone numbers, Physical addresses, Usernames

Adobe: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, *encrypted* password and a password hint in plain text. The password cryptography was poorly done and many were quickly resolved back to plain text. The unencrypted hints also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced.

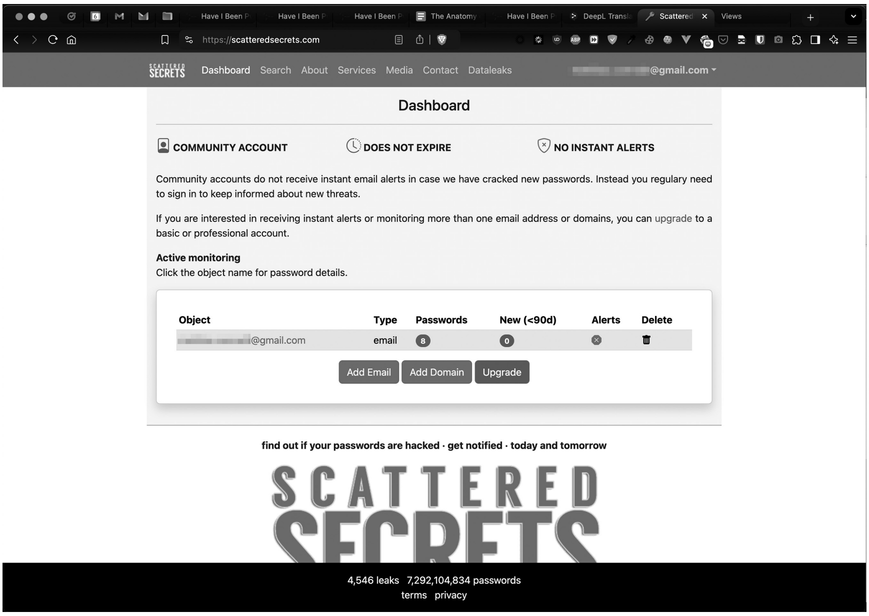
Compromised data: Email addresses, Password hints, Passwords, Usernames

Bitcoin Security Forum Gmail Dump: In September 2014, a large dump of nearly 5M usernames and passwords was posted to a Russian Bitcoin forum. Whilst commonly reported as 5M "Gmail passwords", the dump also contained 123k yandex.ru addresses. Whilst the origin of the breach remains unclear, the breached credentials were confirmed by multiple source as correct, albeit a number of years old.

Compromised data: Email addresses, Passwords

Figure G.3 User screenshot HaveIBeenPwned.[8]

Services like **HaveIBeenPwned** and **ScatteredSecrets** (see Figure G.4) allow you to search their databases to check if your information has been involved in a breach. By entering your email address, you can see whether any of your data was part of past breaches. You can also subscribe for free to be notified if your email address appears in any future breaches they detect.


Have I Been P
Have I Been P
Have I Been P
The Anatomy
Have I Been P
DeepL Transla
Scattered
Views
https://scatteredsecrets.com
SCATTERED SECRETS
Dashboard
Search
About
Services
Media
Contact
Dataleaks
[redacted]@gmail.com
Add Email
Add Domain
Upgrade
SCATTERED SECRETS

Dashboard

COMMUNITY ACCOUNT **DOES NOT EXPIRE** **NO INSTANT ALERTS**

Community accounts do not receive instant email alerts in case we have cracked new passwords. Instead you regulary need to sign in to keep informed about new threats.

If you are interested in receiving instant alerts or monitoring more than one email address or domains, you can upgrade to a basic or professional account.

Active monitoring
Click the object name for password details.

Object	Type	Passwords	New (<90d)	Alerts	Delete
[redacted]@gmail.com	email	8	0	⊗	🗑

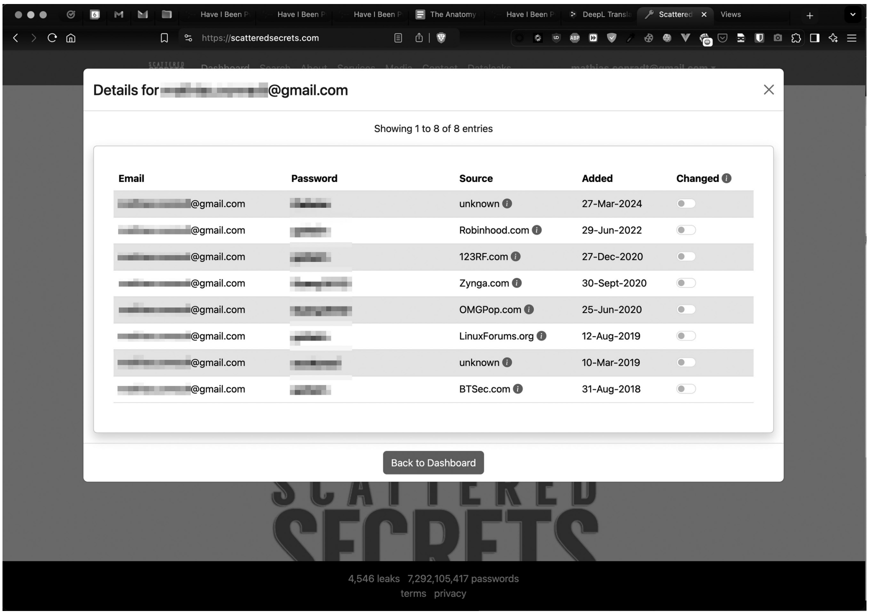
find out if your passwords are hacked · get notified · today and tomorrow

4,546 leaks 7,292,104,834 passwords
terms privacy

Figure G.4 Scattered secrets website.[9]

While **HaveIBeenPwned** shows you the websites and types of compromised data, it doesn't reveal specific data values, such as your passwords.

On the other hand, **ScatteredSecrets** provides an extra layer of detail by showing you the compromised passwords in cleartext, along with the date of the breach. This allows you to review the list and decide if you need to change your passwords on those breached platforms if you haven't done so already (see Figure G.5).


Have I Been P
Have I Been P
Have I Been P
The Anatomy
Have I Been P
DeepL Transla
Scattered
Views
https://scatteredsecrets.com
Dashboard
Search
About
Services
Media
Contact
Dataleaks
Back to Dashboard
SCATTERED SECRETS
4,546 leaks 7,292,105,417 passwords
terms privacy

Details for [redacted]@gmail.com

Showing 1 to 8 of 8 entries

Email	Password	Source	Added	Changed
[redacted]@gmail.com	[redacted]	unknown	27-Mar-2024	○
[redacted]@gmail.com	[redacted]	Robinhood.com	29-Jun-2022	○
[redacted]@gmail.com	[redacted]	123RF.com	27-Dec-2020	○
[redacted]@gmail.com	[redacted]	Zynga.com	30-Sept-2020	○
[redacted]@gmail.com	[redacted]	OMGPop.com	25-Jun-2020	○
[redacted]@gmail.com	[redacted]	LinuxForums.org	12-Aug-2019	○
[redacted]@gmail.com	[redacted]	unknown	10-Mar-2019	○
[redacted]@gmail.com	[redacted]	BTSec.com	31-Aug-2018	○

Figure G.5 Scattered secrets compromised passwords.[10]

Crafting the Attack: The Cyber Attacker's Approach

Phishing and Social Engineering Attacks

Armed with the gathered personal information about the victim, the attacker crafts a message that looks familiar and trustworthy, which they then send to their victim through various channels such as email, messaging apps like WhatsApp or iMessage, SMS, or social media platforms. Instagram, TikTok, Facebook, and X (formerly Twitter) all allow for direct messaging, and attackers might even use the commenting functions on these platforms.

For example, let's say the attacker has identified a victim—a teenager named Mike—who plays the racing game Gran Turismo 7 on PlayStation 5. Mike, a fan of classic cars, has shared screenshots from the game on social media. Many games, including Gran Turismo 7, offer a "photo mode" that allows players to take and share stunning in-game pictures. From Mike's posts, it's clear that he's a big fan of a particular car: the Shelby Cobra Daytona Coupe'64, which is an expensive in-game vehicle.

Additionally, in an older Instagram post, Mike shared a picture of a gaming session where he tagged his friend Jeff, showing both of them in front of the PlayStation console.

With this information, instead of sending a generic, anonymous email or message, the attacker would craft a highly personalized one, such as the example below:

> FROM: ben.doe@sony.com
> TO: mike.jackson89739812@gmail.com
> SUBJECT: PSN gift card for the Shelby Cobra Coupe — Jeff says Hi
> Hello Mike,
> Your friend Jeff, who is also a friend of mine, told me that you're really into Gran Turismo GT, and especially fancy the Shelby Cobra Daytona Coupe'64. He asked me to do you a favor, as I got a couple of PSN gift cards for the DLC (Downloadable Content) as I work at Sony.
> Just use this link to activate the gift card on your PSN account. In case you get asked for any payment information — that's just an age verification they use for coupon codes gifted by Sony employees. You'll see it'll show 0,-
> Enjoy and happy racing :)
> http://psn.couponverify.cc?c=75a6c415-3af4-4f7c-a4f8-dd9ad9393abf
> Cheers,
> Ben Doe

Would you fall for it?

We can probably agree that this email feels very personal and perfectly aligns with Mike's interests. Companies often warn their customers not to fall for phishing attacks. This was the case with Sony, the company in our example, which issued a warning on their blog back in 2010.[11] Even the FBI regularly issues similar warnings[12] to the public.

Phishing and Email Spoofing

For a second victim, a gamer with the handle Hero1985, the attacker tries a slightly different approach. He crafts an email with blue banners and the PlayStation logo, designed to look legitimate. He even sends the email from a fictitious Sony address, like ben.doe@sony.com. Sending an email from a fake address or impersonating someone by using their email as the sender is known as "spoofing."

In the email body, the attacker states that the victim has won a raffle and will receive a coupon code.

Such an email could look like this:

> FROM: noreply@playstation.sony.com
> TO: hero1985@hotmail.com
> SUBJECT: Congrats, Hero1985, you won a PSN gift card worth $250

> Hello Hero1985,
> You are the lucky winner of our monthly raffle at PlayStation. To activate your gift card, simply authenticate at
> http://psn.couponverify.cc?c=75a6c415-3af4-4f7c-a4f8-dd9ad9393abf.
> Congratulations,
> Your PSN team

Psychology Behind Phishing Emails

Phishing emails are designed to manipulate human psychology, targeting emotions and instincts to trick people into taking actions they might not otherwise consider. Here's how they work on a psychological level and what "nerves" they hit:

Familiarity and Trust

Phishers often gather information about their victims and personalize emails to create a sense of familiarity and trust. When an email seems to reference something personal—like a hobby, recent purchase, or a contact you know—it lowers your guard and makes you more likely to believe it's genuine. Just like in our first sample phishing email.

Greed and Excitement

Sometimes phishing emails promise rewards like a prize, a coupon, or a large sum of money. This plays on the recipient's sense of excitement and greed, encouraging them to take quick action to claim the reward, even if it seems too good to be true. The thought of gaining something valuable can cloud judgment. Just like in our second sample phishing email.

Urgency and Fear

Phishing emails often create a sense of urgency or fear, making you feel like something bad will happen if you don't act quickly. For example, an email might claim your account will be locked, or you've missed an important payment. This tactic triggers your natural response to avoid negative outcomes, pushing you to act without thinking carefully.

Authority

Phishers often impersonate trusted organizations or individuals, such as banks, social media platforms, or government agencies, to make the email seem legitimate. By appearing to come from a position of authority, these emails tap into our tendency to trust and follow instructions from people or institutions we see as knowledgeable and powerful.

Curiosity

Many phishing emails use vague or intriguing subject lines to spark curiosity. For example, “You’ve won!” or “Urgent message from your bank!” These messages exploit our natural desire to know more, pushing us to click links or open attachments without thinking about the risks.

By targeting these psychological triggers, phishing emails can manipulate people into giving away sensitive information or clicking on harmful links. Understanding these tactics can help consumers recognize and resist phishing attempts more effectively.

Spoofing vs. Phishing

Spoofing is often mistaken for phishing, though they are distinct concepts. Spoofing involves altering parts of an email to make it appear as if it’s from a different, trusted source.

On the other hand, phishing refers to the act of sending deceptive emails or messages designed to trick recipients into clicking harmful links or downloading malware, which can lead to identity theft, credit card fraud, or other forms of cybercrime.

Spoofing is a technique used in phishing attacks to create a false sense of trust. When an email seems to come from someone familiar, you’re more likely to click a malicious link, open an attachment, or engage with the phishing email.

The following proactive learning objectives should be shared with students. Such actions will assist students in avoiding falling victim to phishing or spoofing scams.

Teaching Tip

Educators should aim to teach students how to:

- Verify the identity of online strangers by cross-referencing with mutual friends to confirm whether the sender is genuine.
- Use OSINT techniques to investigate if someone’s claims about their identity or employment are legitimate, such as checking LinkedIn or social search services like Spokeo.
- Validate social media profiles by examining profile details, conducting reverse image searches, reviewing engagement history, and assessing communication style to identify potential fake accounts.
- Verify if someone truly works at a company by checking professional networks like LinkedIn, examining the email domain, reviewing email headers for Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) authentication, and using email verification services like Hunter.io or Voila Norbert.

- Detect spoofed communication, whether through emails or phone numbers and advise on using secure communication methods like Voice over Internet Protocol services to avoid hidden costs or scams.
- Approach unfamiliar communications cautiously by requesting direct calls using official company channels or performing multiple verification checks before engaging.

Dealing with Online Strangers

If someone refers to a friend of yours, stating that this friend is a mutual one of yours, check back with that friend of yours whether the sender of the suspect message is someone he or she knows.

Using OSINT Techniques Yourself

If the person is claiming to be an adult and working at a certain company, try to google them and see if any profile with trustworthy references comes up. For example, one could check whether this person has a profile on the very popular business platform “LinkedIn” and a job and company he/she claims to be working at. Of course, such profiles can also be faked, even though these platforms nowadays often ask for a mobile phone number verification.

There are also social search services that allow you to enter a name, or an email address, and these services then show you where this name or email address is being used, at how many social media services, how many images can be found related to an email address, etc.

Spokeo[13] is one example of such a social search service. It should be noted that Spokeo’s terms and conditions require its users to be of age 18 and above; hence, such a search should be done by a parent or adult.

When I run a Spokeo Social Search on my email address, it finds it connected to 4+ social networks and 79+ photos online, proof that my email address is often used in various places, and probably has a long history, which is an indicator (although not necessarily) to belong to a legitimate profile.

For people in the United States, the search can even find information about family background, and email authenticity, which is not the case for users in Europe for example, as the data privacy laws in Europe are more restrictive and less information about European citizens is available online by default.

Validating Whether a Social Media Profile Is Fake

Here are some techniques to help validate whether a social media profile is fake:

Check Profile Information

- Start by examining the profile's details. Fake profiles often have incomplete or inconsistent information. Look for a lack of personal details, such as a vague bio, missing location data, or generic profile pictures. Legitimate profiles usually contain more personalized information and consistent details.

Review the Profile Picture

- Fake profiles often use stock photos, images of celebrities, or pictures that seem too polished. You can perform a reverse image search using tools like Google Images[14] or TinEye[15] to see if the profile picture appears elsewhere on the Internet, which might indicate it's stolen or fake.

Analyze Activity and Engagement

- Genuine profiles typically have regular activity, including posts, comments, and interactions with other users. A profile with little to no posts, very few followers, or unnatural engagement (like sudden spikes in followers) can be a red flag. Additionally, check if the posts seem relevant and personal rather than generic or promotional.

Check the Friends or Followers List

- Look at the profile's friends or followers. Fake profiles often have a low number of friends or their friends list might be filled with suspicious or fake-looking accounts. If you see a pattern of connections to other questionable profiles, this is a warning sign.

Assess the Account's History

- Check when the account was created. Fake accounts are often newly created and might lack a substantial history of posts or interactions. A recently created account with a sudden surge in followers or activity could be suspicious.

Evaluate Language and Communication Style

- Pay attention to the language used in the profile's posts and messages. Poor grammar, generic phrases, or an unusual style of communication can indicate a fake profile, especially if it doesn't match the supposed identity of the person.

Observe Direct Communication

- If you receive a message from a profile you suspect is fake, be wary of the content. Scammers often use overly friendly or urgent language, asking for personal information or directing you to click on suspicious links. Authentic profiles typically communicate in a manner consistent with their public persona.

By applying these techniques, you can better determine whether a social media profile is legitimate or potentially fake. Always approach new connections with caution, especially if something about the profile seems off or inconsistent.

Verifying Whether Someone Works at a Company

To verify whether someone works at a company they claim to be an employee of, you can use the following techniques:

LinkedIn and Professional Networks

- Look for the person on other professional networks or industry-specific platforms where they might have a profile listing their current employment. Search for the individual on LinkedIn. A legitimate employee will often have a LinkedIn profile that indicates their current position at the company. Check for consistency between the email domain and the company listed on their LinkedIn profile.

Check the Email Domain

Free Email Providers

- If the email address uses a free email service (like Gmail, Yahoo, or Outlook) instead of a corporate domain, this is a red flag. While some employees might use personal email addresses, official communication from employees is typically sent from a company domain.

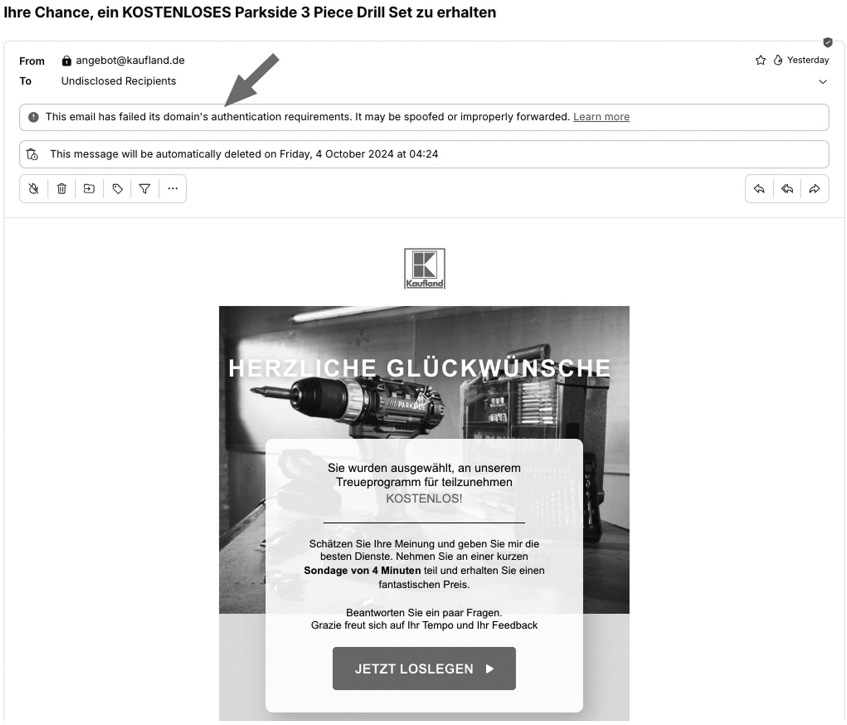
Company Domain

- Look at the part of the email address after the "@" symbol. Legitimate corporate emails usually use the company's official domain (e.g., john.doe@company.com). Verify that the domain matches the official website of the company.

Email Headers

- But that alone is not enough when you receive an email, even when it's coming from a company's official domain at first glance. Technically, a malicious user can send an email from an email address, and domain, they do not own. A cyber attacker could send an email from ceo@microsoft.com or president@whitehouse.gov, and it would show that email address as the sender.

Luckily, good email clients such as Gmail or ProtonMail will recognize that it is a scam and flag it as such; see the examples below of Gmail (see Figure G.6) and ProtonMail (see Figure G.7) identifying fraudulent email address and domain verification.



Ihre Chance, ein KOSTENLOSES Parkside 3 Piece Drill Set zu erhalten

From angebot@kaufland.de

To Undisclosed Recipients

This email has failed its domain's authentication requirements. It may be spoofed or improperly forwarded. Learn more

This message will be automatically deleted on Friday, 4 October 2024 at 04:24

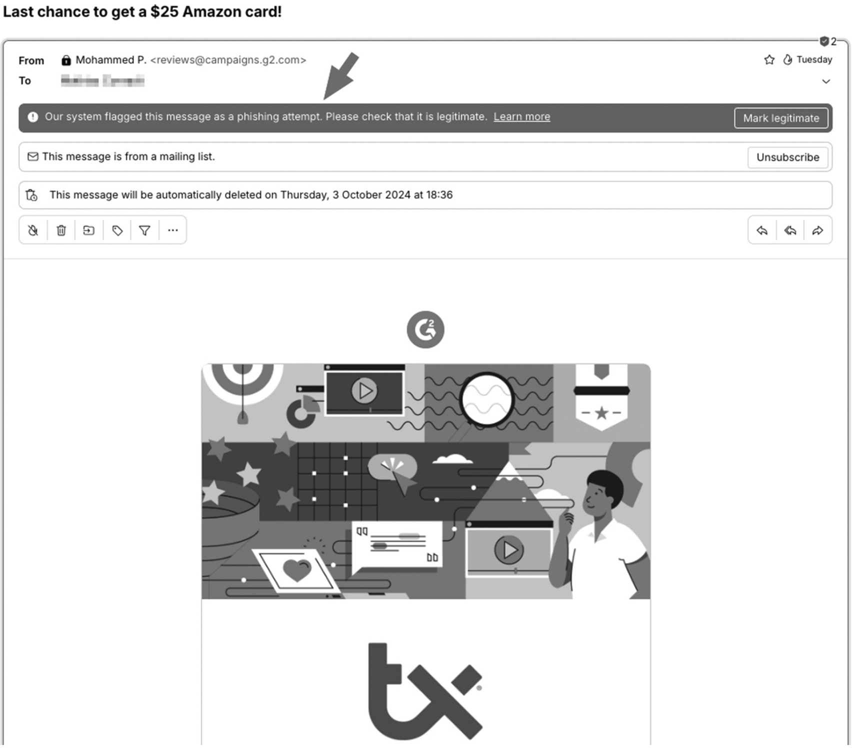
HERZLICHE GLÜCKWÜNSCHE

Sie wurden ausgewählt, an unserem Treueprogramm für teilzunehmen KOSTENLOS!

Schätzen Sie Ihre Meinung und geben Sie mir die besten Dienste. Nehmen Sie an einer kurzen **Sondage von 4 Minuten** teil und erhalten Sie einen fantastischen Preis.

Beantworten Sie ein paar Fragen.
Grazie freut sich auf Ihr Tempo und Ihr Feedback

Figure G.6 Gmail flags an email failing its domain's authentication requirements.[16]



Last chance to get a $25 Amazon card!

From Mohammed P. <reviews@campaigns.g2.com>

To [redacted]

Our system flagged this message as a phishing attempt. Please check that it is legitimate. Learn more

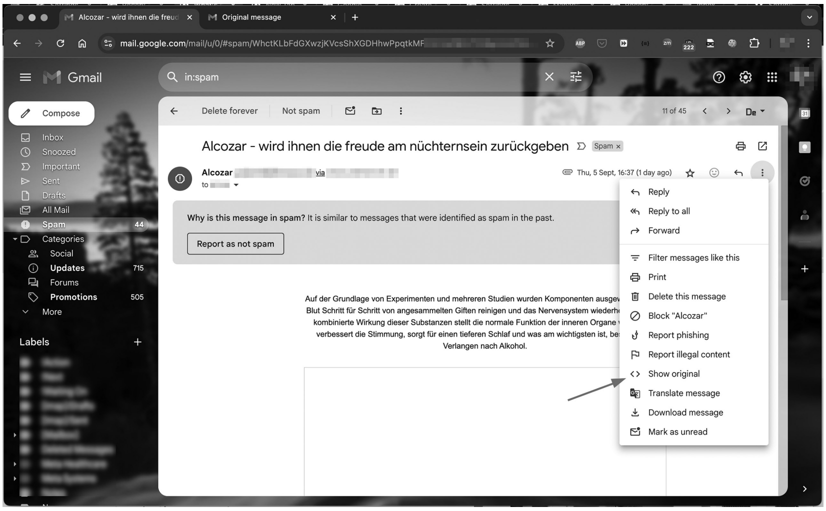
This message is from a mailing list.

This message will be automatically deleted on Thursday, 3 October 2024 at 18:36

Figure G.7 ProtonMail flags a suspicious email as a phishing attempt.[17]

Technically, these good email clients look at the email headers to verify that the email is not spoofed. By default, email clients do not show email headers, as these are quite technical information that are not needed to read the content of an email, however, they are helpful to identify whether an email is legitimate.

In Gmail, the email headers can be viewed by going into the detail view of an email, clicking the "More" menu (3-dots-icon) on the right side of the subject line, and selecting the "Show Original" option from the drop-down menu. This will show the email headers as well as the results of the technical checks that Gmail does here. We will discuss these checks further below (see Figure G.8).



Alcozar - wird ihnen die freude am nüchternsein zurückgeben

Alcozar [redacted] via [redacted]

Thu, 5 Sept, 16:37 (1 day ago)

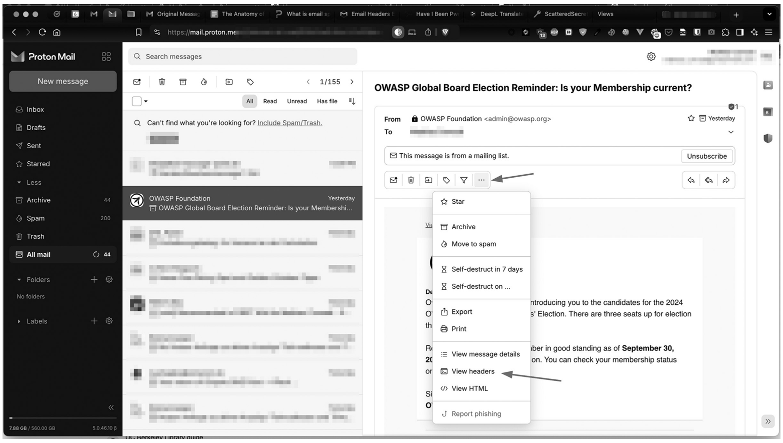
Why is this message in spam? It is similar to messages that were identified as spam in the past.

Auf der Grundlage von Experimenten und mehreren Studien wurden Komponenten ausgev
Blut Schritt für Schritt von angesammelten Giften reinigen und das Nervensystem wiederh
kombinierte Wirkung dieser Substanzen stellt die normale Funktion der inneren Organe
verbessert die Stimmung, sorgt für einen tieferen Schlaf und was am wichtigsten ist, be
Verlangen nach Alkohol.

Alcozar - wird ihnen die freud
Original message
mail.google.com/mail/u/0/#spam/WhctKLbFdGXwzjKVcsShXGDHhwPpqtkMF
Gmail
in:spam
Compose
Inbox
Snoozed
Important
Sent
Drafts
All Mail
Spam 44
Categories
Social
Updates 715
Forums
Promotions 505
More
Labels
Delete forever
Not spam
11 of 45
Spam
Report as not spam
Reply
Reply to all
Forward
Filter messages like this
Print
Delete this message
Block "Alcozar"
Report phishing
Report illegal content
Show original
Translate message
Download message
Mark as unread

Figure G.8 Accessing email headers in Gmail.[18]

In ProtonMail, the email headers can be viewed by going into the detail view of an email, clicking the "More" menu (3-dots-icon), and selecting "View Headers" from the drop-down menu (see Figures G.9 and G.10).



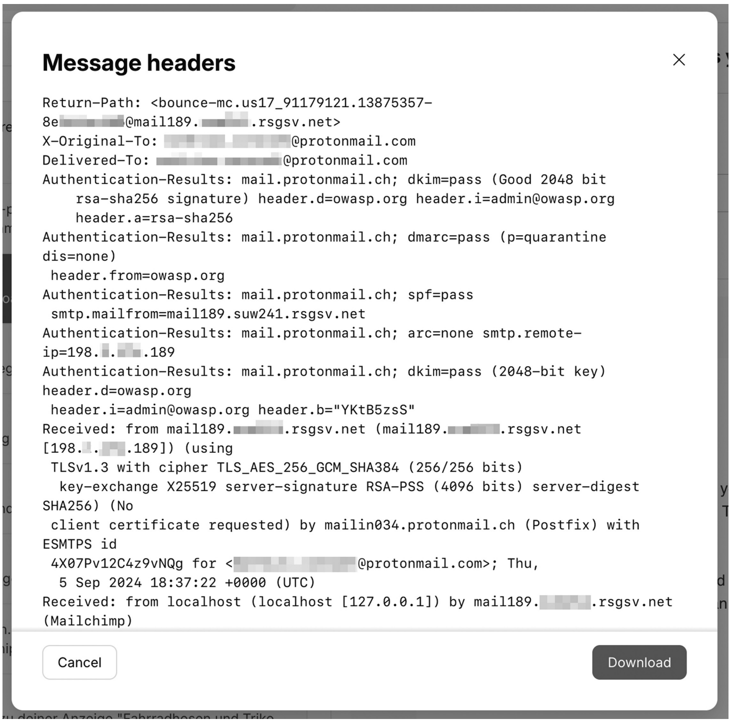
OWASP Global Board Election Reminder: Is your Membership current?

From OWASP Foundation <admin@owasp.org>

This message is from a mailing list.

Original Messag
The Anatomy of
What is email sp
Email Headers
Have I Been Pw
DeepL Translate
ScatteredSecre
Views
https://mail.proton.me
Proton Mail
New message
Inbox
Drafts
Sent
Starred
Less
Archive 44
Spam 200
Trash
All mail 44
Folders
No folders
Labels
Search messages
1/155
All
Read
Unread
Has file
Can't find what you're looking for? Include Spam/Trash.
OWASP Foundation
Yesterday
OWASP Global Board Election Reminder: Is your Membershi...
To
Yesterday
Unsubscribe
Star
Archive
Move to spam
Self-destruct in 7 days
Self-destruct on ...
Export
Print
View message details
View headers
View HTML
Report phishing
ntroducing you to the candidates for the 2024
s' Election. There are three seats up for election
ber in good standing as of September 30,
on. You can check your membership status

Figure G.9 Accessing email headers in ProtonMail.[19]



```
Return-Path: <bounce-mc.us17_91179121.13875357-
8e[redacted]@mail189.[redacted].rsgsv.net>
X-Original-To: [redacted]@protonmail.com
Delivered-To: [redacted]@protonmail.com
Authentication-Results: mail.protonmail.ch; dkim=pass (Good 2048 bit
    rsa-sha256 signature) header.d=owasp.org header.i=admin@owasp.org
    header.a=rsa-sha256
Authentication-Results: mail.protonmail.ch; dmarc=pass (p=quarantine
dis=none)
 header.from=owasp.org
Authentication-Results: mail.protonmail.ch; spf=pass
 smtp.mailfrom=mail189.suw241.rsgsv.net
Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-
ip=198.[redacted].[redacted].189
Authentication-Results: mail.protonmail.ch; dkim=pass (2048-bit key)
header.d=owasp.org
 header.i=admin@owasp.org header.b="YKtB5zsS"
Received: from mail189.[redacted].rsgsv.net (mail189.[redacted].rsgsv.net
[198.[redacted].[redacted].189]) (using
 TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
  key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest
SHA256) (No
 client certificate requested) by mailin034.protonmail.ch (Postfix) with
ESMTPS id
 4X07Pv12C4z9vNQg for <[redacted]@protonmail.com>; Thu,
  5 Sep 2024 18:37:22 +0000 (UTC)
Received: from localhost (localhost [127.0.0.1]) by mail189.[redacted].rsgsv.net
(Mailchimp)
```

Figure G.10 Viewing email headers in ProtonMail.[20]

While inspecting the email header, check the Authentication-Results field (see Figure G.11). If the sender is using SPF, DKIM, or DMARC to authenticate emails, these fields should show “pass”:

spf=pass
dkim=pass
dmarc=pass.

SPF

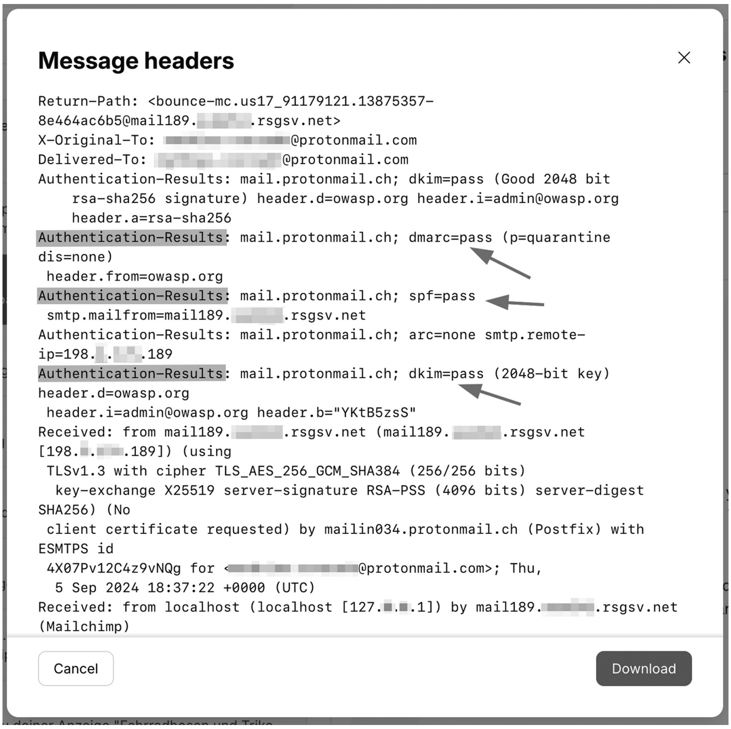
- Confirms that an email originates from an IP address permitted to send messages on behalf of the sender’s domain.

DKIM

- Uses cryptographic methods to verify that the sender’s address and the content of the email remain unaltered during transmission.

DMARC

- Ensures that the domain used in both DKIM and SPF aligns with the domain in the “From” field, providing an important safeguard against email spoofing.

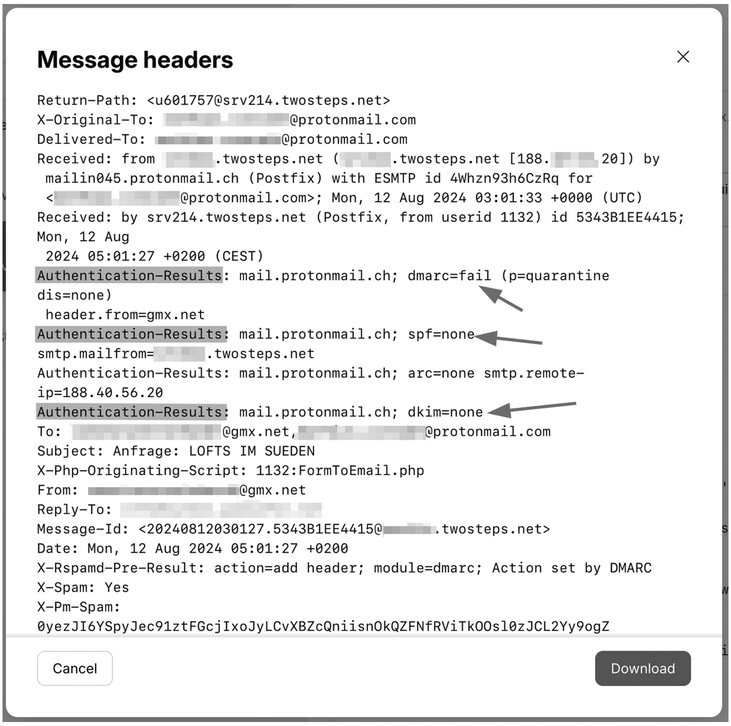


Message headers

```
Return-Path: <bounce-mc.us17_91179121.13875357-
8e464ac6b5@mail189.[redacted].rsgsv.net>
X-Original-To: [redacted]@protonmail.com
Delivered-To: [redacted]@protonmail.com
Authentication-Results: mail.protonmail.ch; dkim=pass (Good 2048 bit
    rsa-sha256 signature) header.d=owasp.org header.i=admin@owasp.org
    header.a=rsa-sha256
Authentication-Results: mail.protonmail.ch; dmarc=pass (p=quarantine
dis=none)
 header.from=owasp.org
Authentication-Results: mail.protonmail.ch; spf=pass
 smtp.mailfrom=mail189.[redacted].rsgsv.net
Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-
ip=198.[redacted].[redacted].189
Authentication-Results: mail.protonmail.ch; dkim=pass (2048-bit key)
header.d=owasp.org
 header.i=admin@owasp.org header.b="YKtB5zsS"
Received: from mail189.[redacted].rsgsv.net (mail189.[redacted].rsgsv.net
[198.[redacted].[redacted].189]) (using
 TLSv1.3 with cipher TLS_AES_256_GCM_SHA384 (256/256 bits)
  key-exchange X25519 server-signature RSA-PSS (4096 bits) server-digest
SHA256) (No
 client certificate requested) by mailin034.protonmail.ch (Postfix) with
ESMTPS id
 4X07Pv12C4z9vNQg for <[redacted]@protonmail.com>; Thu,
  5 Sep 2024 18:37:22 +0000 (UTC)
Received: from localhost (localhost [127.[redacted].[redacted].1]) by mail189.[redacted].rsgsv.net
(Mailchimp)
```

Figure G.11 ProtonMail showing the passed DMARC, SPF, and DKIM checks.[21]

A failed check would look different (see Figure G.12).

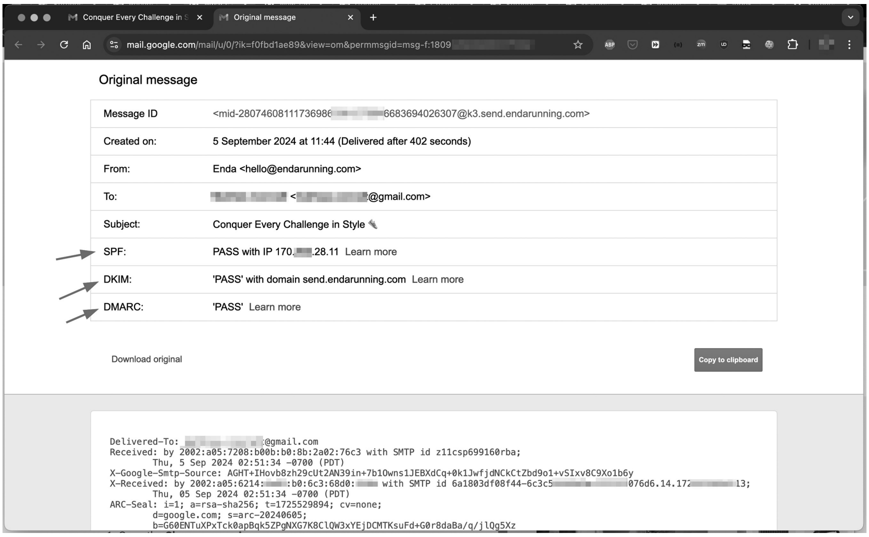


Message headers

```
Return-Path: <u601757@srv214.twosteps.net>
X-Original-To: [redacted]@protonmail.com
Delivered-To: [redacted]@protonmail.com
Received: from [redacted].twosteps.net ([redacted].twosteps.net [188.[redacted]20]) by
 mailin045.protonmail.ch (Postfix) with ESMTP id 4Whzn93h6CzRq for
 <[redacted]@protonmail.com>; Mon, 12 Aug 2024 03:01:33 +0000 (UTC)
Received: by srv214.twosteps.net (Postfix, from userid 1132) id 5343B1EE4415;
Mon, 12 Aug
 2024 05:01:27 +0200 (CEST)
Authentication-Results: mail.protonmail.ch; dmarc=fail (p=quarantine
dis=none)
 header.from=gmx.net
Authentication-Results: mail.protonmail.ch; spf=none
smtp.mailfrom=[redacted].twosteps.net
Authentication-Results: mail.protonmail.ch; arc=none smtp.remote-
ip=188.40.56.20
Authentication-Results: mail.protonmail.ch; dkim=none
To: [redacted]@gmx.net,[redacted]@protonmail.com
Subject: Anfrage: LOFTS IM SUEDEN
X-Php-Originating-Script: 1132:FormToEmail.php
From: [redacted]@gmx.net
Reply-To: [redacted]
Message-Id: <20240812030127.5343B1EE4415@[redacted].twosteps.net>
Date: Mon, 12 Aug 2024 05:01:27 +0200
X-Rspamd-Pre-Result: action=add header; module=dmarc; Action set by DMARC
X-Spam: Yes
X-Pm-Spam:
0yezJI6YSpyJec91ztFGcjIxoJyLCvXBZcQniisnOkQZFNfRViTkOOsl0zJCL2Yy9ogZ
```

Figure G.12 ProtonMail showing the failed DMARC, SPF, and DKIM checks.[22]

Google with its Gmail service shows a positive “PASS” SPF, DKIM, or DMARC to authenticate emails similarly (see Figure G.13).


Conquer Every Challenge in S
Original message
mail.google.com/mail/u/0/?ik=f0fbd1ae89&view=om&permmsgid=msg-f:1809[redacted]
Download original
Copy to clipboard

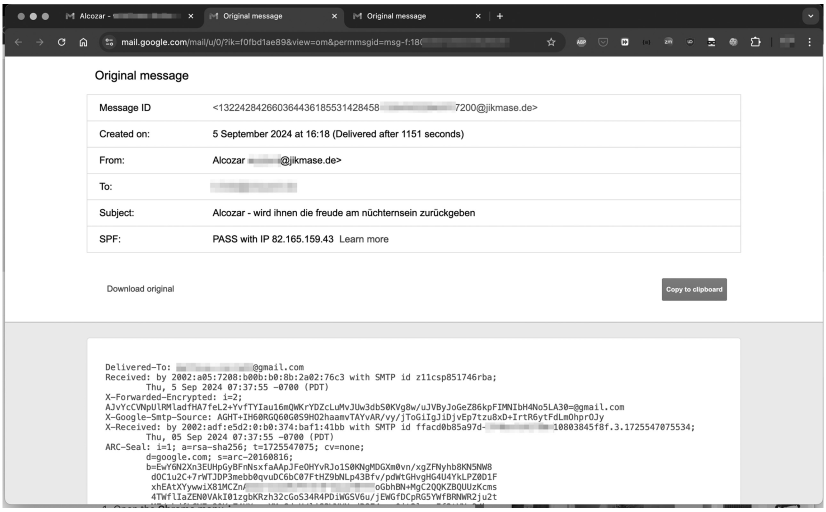
Original message

Message ID	<mid-28074608111736986[redacted]6683694026307@k3.send.endarunning.com>
Created on:	5 September 2024 at 11:44 (Delivered after 402 seconds)
From:	Enda <hello@endarunning.com>
To:	[redacted] <[redacted]@gmail.com>
Subject:	Conquer Every Challenge in Style
SPF:	PASS with IP 170.[redacted].28.11 Learn more
DKIM:	'PASS' with domain send.endarunning.com Learn more
DMARC:	'PASS' Learn more

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a05:7208:b00b:b0:8b:2a02:76c3 with SMTP id z11csp699160rba;
        Thu, 5 Sep 2024 02:51:34 -0700 (PDT)
X-Google-Smtp-Source: AGHT+IHovb8zh29cUt2AN39in+7b1Owns1JEBXdCq+0k1JwfjdNCkCtZbd9o1+vSIxv8C9Xo1b6y
X-Received: by 2002:a05:6214:[redacted]:b0:6c3:68d0:[redacted] with SMTP id 6a1803df08f44-6c3c5[redacted]076d6.14.172[redacted]13;
        Thu, 05 Sep 2024 02:51:34 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1725529894; cv=none;
        d=google.com; s=arc-20240605;
        b=G60ENTuXPxTck0apBqk5ZPgNXG7K8ClQW3xYEjDCMTKsuFd+G0r8daBa/q/jlQg5Xz
```

Figure G.13 Gmail showing the passed DMARC, SPF, and DKIM checks.[23]

If a positive “PASS” DMARC and DKIM checks are missing on this view, it is an indicator that it could be a spam message (see Figure G.14).


Alcozar - [redacted]
Original message
Original message
mail.google.com/mail/u/0/?ik=f0fbd1ae89&view=om&permmsgid=msg-f:18[redacted]
Download original
Copy to clipboard

Original message

Message ID	<132242842660364436185531428458[redacted]7200@jikmase.de>
Created on:	5 September 2024 at 16:18 (Delivered after 1151 seconds)
From:	Alcozar [redacted]@jikmase.de>
To:	[redacted]
Subject:	Alcozar - wird ihnen die freude am nüchternsein zurückgeben
SPF:	PASS with IP 82.165.159.43 Learn more

```
Delivered-To: [redacted]@gmail.com
Received: by 2002:a05:7208:b00b:b0:8b:2a02:76c3 with SMTP id z11csp851746rba;
        Thu, 5 Sep 2024 07:37:55 -0700 (PDT)
X-Forwarded-Encrypted: i=2;
AJvYcCVNpUlRMladfHA7feL2+YvfTYIau16mQWKrYDZcLuMvJUw3dbS0KVg8w/uJVByJoGeZ86kpFIMNIbH4No5LA30=@gmail.com
X-Google-Smtp-Source: AGHT+IH60RGQ60G0S9HO2haamvTAYvAR/vy/jToGiIgJiDjvEp7tzu8xD+IrtR6ytFdLmOhprOJy
X-Received: by 2002:adf:e5d2:0:b0:374:baf1:41bb with SMTP id ffacd0b85a97d-[redacted]10803845f8f.3.1725547075534;
        Thu, 05 Sep 2024 07:37:55 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1725547075; cv=none;
        d=google.com; s=arc-20160816;
        b=EwY6N2Xn3EUHpGyBFnNsxfaAApJFeOHYvRJo1S0KNgMDGXm0vn/xgZFNyhb8KN5NW8
         dOC1u2C+7rWTJDP3mebb0qvuDC6bC07FtHZ9bNLp43Bfv/pdWtGHvgHG4U4YkLPZ0D1F
         xhEAtXYywwiX81MCZnA[redacted]oGbhBN+MgC2QQKZBQUUzKcms
         4TWflIaZEN0VAkI01zgbKRzh32cGoS34R4PDiWGSV6u/jEWGfDCpRG5YWfBRNWR2ju2t
```

Figure G.14 Gmail showing missing DMARC and DKIM checks.[24]

Email Verification Services

Getting back to our sample scenario and the phishing email, where the victim received an email from a “Ben Doe <ben.doe@sony.com>” claiming to work for the company Sony. Regardless of whether the cyber attacker had mentioned the email address or not, we could verify whether this particular “Ben Doe” actually works at the mentioned company.

Use email verification services such as Hunter.io,[25] Voila Norbert,[26] or Verify Email Address[27] to check if the email address is valid and associated with the company’s domain.

These services list known email addresses of users in the company. They might not list all employees, as not everyone is publicly visible on the Internet or does not use social media or business networks like LinkedIn, so they might not appear on platforms like Hunter.io, as they rely on publicly available information from the Internet.

Try it out yourself with this example URL: https://hunter.io/discover/170034?domains=sony.com&filters_changed=1.

However, even if we do not find “Ben Doe” on such platforms, we can still derive the email pattern that the company uses.

Some companies use an email address pattern of firstname.lastname@company.com, others use lastname@company.com, while others use the first letter of the first name and the full family name, like flastname@company.com.

Knowing the email pattern helps us to craft an email to the person in question. Send a polite and professional email to the address in question, asking for confirmation of the person’s role and association with the company. If the email bounces back with an “Unable to deliver” error message, we would then know that the email address does not exist.

If the email does not bounce back but the recipient does not know anything about any coupon codes mentioned in the phishing email and has not heard your name before, we can also be sure that the cyber attacker impersonated that employee without their knowledge.

Another way of verifying the legitimacy of a person is to request a call. Suggest setting up a call or meeting using the company’s official communication channels. Legitimate employees are usually comfortable with this, while someone misrepresenting themselves may avoid direct communication.

In case a cyber attacker approaches you via WhatsApp or SMS or leaves a phone number in some way: Do not initiate a regular phone call to a number you don’t know, use VoIP services like WhatsApp, Zoom, Webex, or Microsoft Teams, as unknown numbers dialed over the phone system may incur additional hidden costs.

A final word on “spoofing,” just like email addresses, can be spoofed as explained above, phone numbers can also be spoofed similarly. Cyber attackers can use apps like SpoofCard and others[28] to make an incoming phone call look as if it is coming from a nearby location or even from a person you know.

These apps often have additional features to allow the distortion of the caller's voice, changing the pitch or turning a male into a female voice and vice versa.

Using the methods discussed above, you can more effectively determine if someone genuinely works at the company they claim to be associated with. If multiple checks raise doubts, it's safer to be cautious and avoid sharing sensitive information with individuals whom you cannot validate.

Summary

In conclusion, understanding the methods cyber attackers use to gather information and craft personalized phishing attacks is essential for protecting oneself in today's digital landscape.

By recognizing the tactics employed—such as OSINT, social engineering, and email spoofing—individuals can better safeguard their personal information, especially when interacting on social media and gaming platforms. It is crucial to adopt cyber-safe online practices, such as verifying the legitimacy of communications, managing digital footprints, and using tools to detect and respond to potential breaches.

Ultimately, being vigilant and informed can significantly reduce the risk of falling victim to targeted cyberattacks.

∝

About the Author

Mathias Conradt

Principal Solutions Engineer at Snyk, OWASP Member

Mathias brings over 20 years of experience in software engineering and project management, with a strong focus on open-source technologies. He was a Visiting Professor in Android development at the University of St. Joseph in Macau, China, and ran his own boutique software development company with offices in Germany, Hong Kong, and the United States for more than 15 years before transitioning into the cybersecurity industry.

Currently based in Stuttgart, Germany, Mathias has worked in Identity & Access Management at Auth0 and now leads technical presales in the DACH region at Snyk, specializing in developer-focused applications and cloud security. He is also a frequent speaker at information security industry events and an author of professional articles on application security and cybersecurity.

∝

The authors wish to thank Mathias for his contribution to our book and our efforts to teach cyber-safe practices to students, and all those who teach and care for students, globally.

Notes

1 Further information on Just Delete Me may be found at https://justdeleteme.xyz.
2 JustDeleteMe, September 6, 2024, Figure G.1, “JustDeleteMe Author’s Personal Screenshot Home Page,” https://justdeleteme.xyz/#amazon, retrieved September 6, 2024, used with permission.
3 Further information on Incogni may be found at https://incogni.com.
4 Further information on DeleteMe may be found at https://joindeleteme.com.
5 Further information on Breachsense may be found at www.breachsense.com/breaches/2024/september/.
6 Further information on HaveIBeenPwned may be found at https://haveibeenpwned.com/.
7 BreachSense, September 6, 2024, Figure G.2, “Data Breaches in 2024,” Breachsense screenshot, www.breachsense.com/breaches/2024/september/, retrieved September 6, 2024, used with permission.
8 HaveIBeenPwned, September 6, 2024, Figure G.3, “HaveIBeenPwned Screenshot,” https://haveibeenpwned.com/, retrieved September 6, 2024, used with permission.
9 Scattered Secrets, September 6, 2024, Figure G.4, “Scattered Secrets Website,” https://scatteredsecrets.com, retrieved September 6, 2024, used with permission.
10 Scattered Secrets, September 6, 2024, Figure G.5, “Scattered Secrets Compromised Passwords,” https://scatteredsecrets.com, retrieved September 6, 2024, used with permission.
11 PlayStation.Blog, April 21, 2010, “WARNUNG: Vorsicht vor Phishing-Mails im PSN” [German], https://blog.de.playstation.com/2010/04/21/warnung-vorsicht-vor-pishing-mails-im-psn/, retrieved September 6, 2024.
12 ComputerWoche, September 5, 2011, “PlayStation Scam Makes FBI Warning List,” www.computerwoche.de/article/2629824/playstation-scam-makes-fbi-warning-list.html, retrieved September 6, 2024.
13 Further information on Spokeo Social Search (Reverse Email Lookup) may be found at www.spokeo.com/email-search.
14 Further information on Google Images may be found at https://images.google.com/.
15 Further information on TinyEye may be found at https://tineye.com/.
16 Google, September 6, 2024, Figure G.6, “Gmail Flags an Email Failing Its Domain’s Authentication Requirements,” author’s personal screenshot, https://mail.google.com, retrieved September 6, 2024.
17 ProtonMail, September 6, 2024, Figure G.7, “ProtonMail Flags a Suspicious Email as Phishing Attempt,” author’s personal screenshot, https://mail.proton.me, retrieved September 6, 2024.
18 Google Gmail, September 6, 2024, Figure G.8, “Accessing Email Headers in Gmail,” author’s personal screenshot, https://mail.google.com, retrieved September 6, 2024.
19 ProtonMail, September 6, 2024, Figure G.9, “Accessing Email Headers in ProtonMail,” author’s personal screenshot, https://mail.proton.me, retrieved September 6, 2024.
20 ProtonMail, September 6, 2024, Figure G.10, “Viewing Email Headers in ProtonMail,” author’s personal screenshot, https://mail.proton.me, retrieved September 6, 2024.
21 ProtonMail, September 6, 2024, Figure G.11, “ProtonMail Showing the Passed DMARC, SPF, and DKIM checks,” author’s personal screenshot, https://mail.proton.me, retrieved September 6, 2024.
22 ProtonMail, September 6, 2024, Figure G.12, “ProtonMail Showing the Failed DMARC, SPF, and DKIM checks,” author’s personal screenshot, https://mail.proton.me, retrieved September 6, 2024.
23 Google Gmail, September 6, 2024, Figure G.13, “Gmail Showing the Passed DMARC, SPF, and DKIM checks,” author’s personal screenshot, https://mail.google.com, retrieved September 6, 2024.

24 Google Gmail, September 6, 2024, Figure G.14, “Gmail Showing Missing DMARC and DKIM Checks,” author’s personal screenshot, https://mail.google.com, retrieved on September 6, 2024.

25 Further information on Hunter.io may be found at https://hunter.io/.

26 Further information on Voila Norbert may be found at https://www.voilanorbert.com/email-finder/.

27 Further information on Verify Email Address may be found at https://www.verifyemailaddress.org/email-validation.

28 Further information on the Best 5 Call Spoofing Apps in 2024 may be found at www.imyfone.com/change-location/best-call-spoof-app/.

Appendix H: Cyber Safety and the Online World Safe/Unsafe People & The Tricky Person

Mental Wellness Strategies for Grades 7 & 8

Written by Mandy Schumacher, T-LAC, and Stephanie Nilsen, Ph.D., T-LAC

As we discussed in other areas within the chapters of this book, online safety concerns can lead to online risky actions by our exploring early teens, and often unintentionally. Online chats can lead to sexting, which may lead to other actions such as sextortion or requests to move from online conversations to in-person meetings. The person online isn't who they said they were. The sextortion isn't stopping as promised with more pictures. As each step escalates, the victim may feel that they have let everyone down. Parents and other family members will be so disappointed. They are embarrassed and feel shame. To whom can they share this? Will the authorities be involved? These online activities and traps lead to feeling overwhelmed and anxious.

> The authors and contributors are not mental health professionals, and the following section is not mental health or medical advice. It is presented to teachers as helpful information and to create awareness of the cue's students may display when experiencing well-being trials and offers suggestions for action. The information contained is not a substitute for the knowledge, skills, and judgment of a qualified mental health professional. These concepts and responses are designed to make you a trusted person to the students, someone who cares about them and to whom they can turn when in need.
>
> If you see (or if you feel) safety concerns, reach out to a crisis line by dialing or texting 988 immediately.

When considering the impact of online exposure on the minds and emotional well-being of our adolescents, it is imperative to understand a few ins and outs of the developing brain. When considering unsafe and tricky persons online, this psycho-education is incredibly relevant. During children's preteen years, studies support that oxytocin and dopamine multiply in a part of the brain called the ventral striatum, making them extra sensitive to attention and admiration from others.[1] One can imagine how this deep desire for approval and connection may make adolescents more susceptible to risks online. The tricky person may use grooming tactics that prey on this endearing and inherent adolescent desire to belong, feel seen, and be accepted. As safe, loving, and secure adults in this adolescent's life, it is our responsibility to teach and monitor safe connections online.

Proactive Support

With safe use, teens can *enhance* their mental well-being by promoting healthy socialization.[2] Teens can develop long-lasting friendships, nurture their creativity, and utilize Internet resources to expand their knowledge of the world around them. To allow adolescents the best chance at safe and beneficial use, an adult can:

1. Go Beyond Discussions around Screen Time: Become curious about your student's use of technology through compassionate two-way discussions and show genuine interest in their online platforms of choice. Example:

> Many of you have shared that you play online games like Fortnite! How many of you have played that game? What skin do you have? Have you ever chatted with someone you don't know? If so, did they ask about details of your life that did not have to do with gameplay? How do you know the person is safe?

2. Teach Online and Social Media Literacy: Teaching online literacy for this age group can include discussing the permanency of online data, avoiding posting personal information/sexting, explaining warning signs of online predators, identifying trusted adults, and showing them how to set up privacy controls and how to turn off location settings on apps, discuss cyberbullying, and bring awareness to illegal activities online (US Dept of Homeland Security). Conversations around social media literacy are also imperative. These discussions can include education about social media not being a portrayal of reality and the power of comparison, how to identify a source as trustworthy in an effort not to spread misinformation, preventing conflicts on social media, and teaching critical thinking when it comes to discrimination against marginalized groups.[3]
3. Set Appropriate Boundaries and Monitor Use: Families can create family media use plans collaboratively to support boundaries around screen use. This can also be mimicked in a classroom/school setting. For example, screen-free spaces, screen-free times, and one-screen-at-a-time rules can support an adolescent with safe/healthy online exposure, and modeling appropriate use.[4]

Warning Signs and Assessment

If you suspect the teen has been involved in a risky exposure or a student's mental health has been compromised due to unhealthy online use, here are a few warning signs to be on the lookout for:

1. Secretiveness/Deception: Behaviors of deception could include misuse of passwords or creating fake "burner" accounts. These deceptive behaviors can be assessed using parent reports on the nine-item Social Media Disorder Scale (SMDS).[5]
2. Emotional and Behavioral Changes: A few emotional and behavioral changes to be aware of which are also part of the nine-item SMDS include preoccupation with social media, withdrawal, struggle with tolerance (increased irritability, anxiety, irritation), displacement (regularly neglecting other activities to engage online), and common arguments with others about screen use, using social media to escape negative emotions.
3. Unmet Basic Needs: Sometimes warning signs can be observable. Adults in the teen's life can be on the lookout for a change in appetite, eating habits, or sleep hygiene. If online activity results in neglect of the adolescents' basic needs, it may be time to discuss this with your teen.
4. Comparison Statements/Noticeable Changes in Self-Esteem: If a teen you work with often uses comparison statements about peers/celebrities or begins verbalizing self-defeating statements, this could be an indication of unhealthy social media consumption. Facilitating healthy, open conversations around what accounts teens follow and the impact it has on their self-esteem is essential.
5. Disordered Eating Habits: Along with comparison statements, it is important to be aware that a teen's social media consumption can exacerbate hurtful comparisons to peers or celebrities online with body types the teen may prefer. There are clear patterns of association between social media use and disordered eating cognitions and behaviors.[6] Behaviors of disordered eating vary, but can include distorted body image, fixation on appearance, extreme dieting or overeating, and an avoidance of eating socially. You may notice a teen excessively exercising, spending a lot of time in the bathroom, or even going to the bathroom immediately following eating.[7] Other signs of disordered eating may include lethargy or tiredness, increased difficulty with concentration, frequent feeling cold even in warmer temperatures, and dizziness or fainting.
6. Suicidal Ideation[8]/Self-Harm Behaviors: When assessing if a teen is struggling with suicidal ideation, pay attention to the following:
   - Talking about: Wanting to die, great guilt or shame, and being a burden to others.
   - Feeling: Empty, hopeless, trapped, or having no reason to live, extremely sad, more anxious, agitated, or full of rage, unbearable emotional or physical pain.

- Changed Behavior: Making a plan or researching ways to die, withdrawing from friends, saying goodbye, giving away important items, or making a will, taking dangerous risks such as driving extremely fast, displaying extreme mood swings, eating or sleeping more or less, using drugs or alcohol more often.[9]

Self-harm warning signs can look like the following:

- Mood Changes: Drastic or frequent changes in mood merit a check-in with your teen.
- A Trigger Event: Sometimes self-harm is triggered by an adverse event. If you are aware your teen has experienced something emotionally impactful, check in with them and leave the door open for open communication.
- Fascination with Self-harm: This includes reading or watching videos online. This goes back to monitoring use and having compassionate and curious conversations with teens about what they are consuming online.
- Isolation: Shutting themselves off from family and friends can also be a warning sign and reason for concern for your teen.[10]

Reactive/Supportive Responses

If the warning signs are apparent and you suspect and/or confirm risky online behavior (i.e., a student discloses a connection with an unsafe/tricky person, reveals a compromising photo has been posted, etc.), a teacher should consider following actions or supportive next steps:

1. Parent Involvement: If disclosure of unsafe online use is reported to a teacher, then sharing with a parent may be necessary. Encouraging the student to find a collaborative, safe, and supportive way to share information will aid in building trust. Though you may not have a choice *if* sharing the information is necessary, it can be empowering to the student to choose *how* to share it with a parent (i.e., with or without the teacher present, which parent to share with first, in person/over the phone, etc.).
2. Seek Professional Support: If an adolescent's mental health has been compromised or many of the warning signs previously discussed are apparent, the safe adult should consider seeking referrals for mental health therapy. If the teen shows active compromised safety or endorses suicidal ideation/self-harm behavior, reach out to a crisis line. **Dialing or texting 988** will connect your teen with a trained crisis counselor. This line is available 24/7.
3. Report the Problem: Unsafe or tricky persons can be reported on the **Know2Protect Tip Line** at 833-591-Know (5669). All information received via the Tipline will be reviewed by appropriate personnel and referred to Homeland Security Investigations. If the adolescent endorses unsafe exposure, sexual exploitation, or interaction with an unsafe person, then a call to 911 is appropriate.

About the Authors

Mandy Schumacher

Mandy has experience working with children, families, adolescents, and adults in both the clinical and school setting. An LGBTQ+ affirming clinician who always prioritizes honoring all cultural backgrounds. Mandy's practice focuses on identifying maladaptive patterns, examining roles within family systems, healing wounded relationships with self and others, and processing trauma. Mandy is passionate about Social-Emotional Learning and play therapy for children. "Whether struggling with depression, anxiety, dependency, or troubled relationships – I will always come from a place of empathy and hold you in the highest regard."

Mandy earned her Elementary Education Degree at the University of Wyoming, teaching elementary school for 3 years in Arizona, and then spending 1 year traveling the United States, working for National Geographic Learning. Mandy then earned her Master's in Counseling from Arizona State University.

Stephanie Nilsen

From teaching kindergarten to higher education and on to becoming a counselor, Mandy has watched and worked with humans of all ages and all stages as they learn to face challenges and experience growth. Overcoming is a human endeavor, and relationships are the foundation for learning new ways to face whatever is standing in your way.

Stephanie works with individual adults (from teens to seniors), families, and children to help identify barriers to development and focus on utilizing the strategies that will best facilitate positive change. Using trauma-informed approaches that begin where individuals are to help promote success and positive change can help to build skills and work through depression, anxiety, trauma, relationships, and more.

Stephanie started in Early Childhood Education teaching in Preschool, Kindergarten, and Elementary grades, particularly in early intervention and special education realms, continuing to a second Master's in Mental Health Counseling with an emphasis in trauma, and her Doctorate in Infant and Early Childhood Development with an emphasis in Mental Health and Developmental Disorders.

∝

The authors wish to thank Stephanie and Mandy for their contribution to our book and to help keep students safe online.

Additional References

Abrams, Z., 2022, "What Neuroscience Tells Us about the Teenage Brain," https://www.apa.org/monitor/2022/07/feature-neuroscience-teen-brain.

National Eating Disorders Association, n.d., "Media and Eating Disorders," https://www.nationaleatingdisorders.org/media-and-eating-disorders/#sources.

Stein, A., 2024, "Eating Disorders in Teens: Warning Signs and Treatment Options for Your Child," https://www.uchicagomedicine.org/forefront/pediatrics-articles/eating-disorders-in-teens-Warning-signs-and-treatment-options.

Zhang, J., Wang, Y., Li, Q., & Wu, C., 2021, "The Relationship between SNS Usage and Disordered Eating Behaviors: A Meta-Analysis," *Frontiers in Psychology*, 12, 641919. https://doi.org/10.3389/fpsyg.2021.641919.

Notes

1 Abrams, Z., 2023, "Why Young Brains Are Especially Vulnerable to Social Media," https://www.apa.org/news/apa/2022/social-media-children-teens, retrieved November 2, 2024.

2 Weir, K., 2023, "Social Media Brings Benefits and Risks to Teens: Psychology Can Help Identify a Path Forward," https://www.apa.org/monitor/2023/09/protecting-teens-on-social-media, retrieved November 2, 2024.

3 Prinstein, M., May 9, 2023, "Keeping Teens Safe Online," Keeping Teens Safe on Social Media: What Parents Should Know to Protect Their Kids, retrieved November 6, 2024.

4 Kids Online Health & Safety Task Force, n.d., "Online Health and Safety for Children and Youth: Best Practices for Families and Guidance for Industry," https://www.ntia.gov/sites/default/files/reports/kids-online-health-safety/2024-kohs-report.pdf, retrieved November 2, 2024.

5 Austermann, M., Tomasius, R., Pashke, K., February 6, 2021, "Assessing Problematic Social Media Use in Adolescents by Parental Ratings: Development and Validation of the Social Media Disorder Scale for Parents (SMDS-P)," https://pmc.ncbi.nlm.nih.gov/articles/PMC7914646/, retrieved November 2, 2024.

6 Wilksch, M., O'Shea, A. Ho, P., Byrne, S., & Tracey, W., 2019, "The Relationship between Social Media Use and Disordered Eating in Young Adolescents", https://pubmed.ncbi.nlm.nih.gov/31797420/, retrieved November 6, 2024.

7 Ehmke, R., 2023, "When to Worry about an Eating Disorder," https://childmind.org/article/when-to-worry-about-an-eating-disorder/, retrieved November 2, 2024.

8 Additional information regarding suicide and suicide ideation may be found in Appendix I.

9 (n.a.), July 31, 2024, Kaiser Permanente, "Warning Signs of Suicide in Children and Teens," https://healthy.kaiserpermanente.org/health-wellness/health-encyclopedia/he.warning-sigNs-of-suicide-in-children-and-teens.ty6090, retrieved November 6, 2024.

10 (n.a.), (n.d.), "Warning Signs of Suicide (NIMH)," https://www.nimh.nih.gov/health/publications/warning-signs-of-suicide, retrieved November 2, 2024.

Appendix I: Online Use — Teen Well-being and Mental Health

As discussed in other areas within the chapters of this book, online safety concerns can lead to often unintentional risky online actions by our exploring teens. Online chats can lead to sexting, which may lead to other actions such as sextortion or requests to move from online conversations to in-person meetings. The person online isn't who they said they were. The sextortion isn't stopping as promised with more pictures. As each step escalates, the victim may feel that they have let everyone down. Parents and other family members will be so disappointed. They are embarrassed and feel shame. To whom can they share this? Will the authorities be involved? These online activities and traps lead to feeling overwhelmed and anxious.

> The authors and contributors are not mental health professionals, and the following section is not mental health or medical advice. It is presented to teachers as helpful information and to create awareness of the cue's students may display when experiencing well-being trials and offers suggestions for action. The information contained is not a substitute for the knowledge, skills, and judgment of a qualified mental health professional. These concepts and responses are designed to make you a trusted person to the students, someone who cares about them and to whom they can turn when in need.
>
> If you see (or if you feel) safety concerns, reach out to a crisis line by dialing or texting 988 in the US or locate a global resource here - https://unitedgmh.org/support/.

Suicide — Well-Being and Mental Health for Grades 7 & 8

Written by Rikki Turner, Ed.D.

We can see how online activities and missteps lead to feeling overwhelmed and anxious. These feelings cause many to believe that there is no way out. This thinking spirals to thoughts of harming themselves or of suicide as the only way to escape.

It is important to talk about well-being directly with teens. Although they may not display signs causing immediate concern, opening this discussion builds the relationship whether for them, or their friends and family, who they know are at this level of distress. It lets them know that they are important, their concerns are important, and they can come to you — now or in the future. Many teens may not exhibit overt signs of distress. Instead, they may have subtle changes in behavior, disposition, become angry or lethargic, or there may be changes in their class work and school participation.

Rikki Turner, Ed.D., has made it her mission to reduce the number of suicides[1] by teaching others practical, accessible strategies to intervene. During her years as a higher education administrator and serving on behavior intervention teams, she was often called upon to intervene with suicidal students.

> As Turner often notes, she is the "thinky-speaky" doctor and not the medical doctor. Turner's contribution is not mental health or medical advice. It is presented to teachers as helpful information and to create awareness of the cue's students may display when experiencing mental distress. This section is designed to empower you as a trusted person to the students, someone who cares about them, and to whom they can turn when in need.
>
> If you see (or if you feel) safety concerns, reach out to a crisis line by dialing or texting 988 immediately.

Turner's concepts and suggested responses are backed by mental health research and from 20 years of experience working with students in crisis. In her role as an administrator, her campus experienced a very sharp and heartbreaking increase in suicides and suicide attempts. When the behavioral intervention team she served on spoke with the faculty of those students, they all had noticed something wasn't right with the students, but none of them did anything to try and help the students. This was the impetus to her dissertation study and investigation into why faculty may not intervene (Figure I.1).

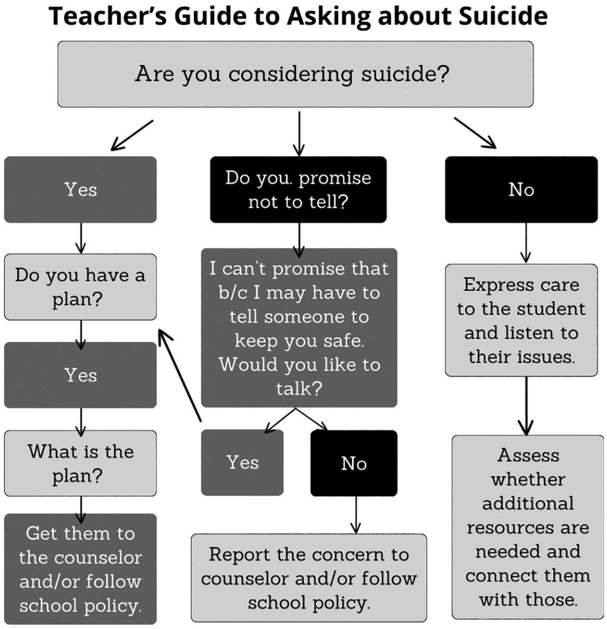

Teacher's Guide to Asking about Suicide
Are you considering suicide?
Yes
Do you. promise not to tell?
No
Do you have a plan?
I can't promise that b/c I may have to tell someone to keep you safe. Would you like to talk?
Express care to the student and listen to their issues.
Yes
What is the plan?
Yes
No
Assess whether additional resources are needed and connect them with those.
Get them to the counselor and/or follow school policy.
Report the concern to counselor and/or follow school policy.

Figure I.1 Teacher's guide to asking about suicide.[2]

Too often, I've heard from principals, teachers, and counselors who believe common myths about mental health—such as the idea that suicide prevention programming might put the idea of suicide into students' minds, or that only low-achieving students need support. But the truth is, online pressures affect all students, from those excelling academically to those who may be struggling. Your job isn't to solve these problems alone, but rather to recognize when a student needs help and to ensure they get it before it's too late (Table I.1).

According to Turner, it is good practice to establish a code word. This will remove the stigma of asking for help, or of a person who needs immediate help. Turner recommends a word that is outlandish and not a usual word; it is not in everyday language. Whatever the word you choose, let them know they can text you, email it to you, or say it in conversation and it will alert you that you need to talk.

Table I.1 The Suicide Lady Podcast, Episodes 2 and 3

SITUATION	CONTEXT	RESPONSE TO TEEN	FEEDBACK
Myth in talking about suicide gives them the idea.	Everyone knows what it is and how people do it. Why then have they not? They don't WANT to!	Ask them directly if they are considering suicide. Ask earnestly and with empathy, such as follows: "I am worried about you and care about you. Have you had any thoughts of Suicide?"	This discussion does not make the situation worse. It opens the discussion and establishes you as a trusted person who cares about their well-being.
They say, "Will you not tell anyone?"	Let them know you cannot make this promise — it is all about them and their safety. Reassure them that even if you must tell someone, you tell them who you are telling before you do.[3]	Let them know you will continue to care for them, listen, and to be there for them through the process. As a best practice in full transparency, you may indicate, "I can't promise that I won't tell anyone because if you are in danger, I want to keep you safe. However, I can tell you every step of the way what I am doing and why I am doing it."	The focus needs to remain on them and their safety, no one else.
They say "Yes, I have thought about it."	It is usually not about wanting to die, but about not wanting to hurt anymore and feeling out of options.	You are interested in them; it shows them you are concerned. You recognize something is off. "I am worried about you because xyz. What could be causing this?"	• Ask without judgment. • … • Do not explain why they shouldn't or what they have to live for. • Do not explain that others have it worse. • Listen. Just listen.
		Ask them if they have a plan. Again, you are interested in them, using concerned words and tone. "Thank you for trusting me with this. Are these thoughts that come and go or do you have a plan?" Allow them to talk.	Asking if they have a plan is a helpful intervention tool. This tells you how emergent the situation is. Often teens just feel like they have no one who will listen. Don't try to fix it — listen without interruption and then reflect on what you heard to ensure you understand.
They say "Yes, I have a plan/know what I will do."		Ask gently and without judgment, "What is your plan?" This information is needed to help keep them safe. Ask for specifics — what is your plan, how, where, when?	Offer to go with them to seek help while honoring your school's policy. This could mean walking them to the counselor's office. Know the phone number 988 — the suicide prevention hotline.

(*Continued*)

Table I.1 (*Continued*) The Suicide Lady Podcast, Episodes 2 and 3

SITUATION	CONTEXT	RESPONSE TO TEEN	FEEDBACK
They may again ask you not to tell anyone.	Let them know you cannot make this promise — it is all about them and their safety.	Let them know you are only interested in their safety. You want to help them, and you need to know how to do that.	We never want to make a promise we can't keep to a student. This diminishes trust, and we know that previous suicide attempts are one of the strongest predictors of a future suicide attempt.[4]
They say, "No." with no further information.	It's defensive, which is okay. Reaffirm your care and concern for them.	Here's why I am concerned … and state or restate your observations.	Let them know you are a safe person for them and that you are there for them. Often, they just need someone to listen to them.

Turner, R., "The Suicide Lady Podcast," Episodes 2 and 3, The Suicide Prevention Lady Podcast | Podcast on Spotify.

About the Author

Rikki Turner, Ed.D.

Rikki spent years as a higher education administrator and served on behavior intervention teams. She was often called upon to intervene with suicidal students. This experience led her to focus her dissertation study on faculty's willingness to intervene with suicidal students. She has made it her mission to reduce the number of suicides by teaching others practical, accessible strategies to intervene.

Rikki is a state and regional award-winning speaker and presenter. Using humor and personal stories, her keynotes draw attendees of all ages. She is actively involved in the *National Association of Student Personnel Administrators (NASPA)*, the *Association for College Personnel Educators (ACPA)*, the *American Association of Suicidology (AAS)*, and the *JED Foundation*, among others. She is also engaged in ongoing research to further understand suicidal behavior and effective intervention strategies. Rikki is the Founder of Still You Rise.

The authors wish to thank Rikki Turner for her contribution to our book and our efforts to teach cyber-safe practices to students and uphold their well-being and mental health.

∝

The authors wish to thank Rikki for her contribution to our book to help keep students safe online, and for her work to offer all those who teach and care for students with dialogs to address and reduce the number of teen suicides.

Additional Resources

June 4, 2024, U.S. Centers for Disease Control and Prevention (CDC), "Suicide Prevention Resources for Action," Suicide Prevention Resource for Action | Suicide Prevention | CDC.

U.S. Department of Health and Human Services, 2024 National Strategy for Suicide Prevention, 2024 National Strategy for Suicide Prevention | HHS.gov.

Notes

1 References to suicide should be "suicide, suicidal ideation, thoughts of suicide, or death by suicide" as options. The mental health community strongly advocates against using "commit" with suicide.
2 Figure I.1. "Teacher's Guide to Asking about Suicide," Rikki Turner, used with permission.
3 Refer to Chapter 3 Mandatory Reporters content.
4 Bostwick, J. M., Pabbati, C., Geske, J. R., McKean, A. J., 2016. "Suicide Attempt as a Risk Factor for Completed Suicide: Even More Lethal Than We Knew," *The American Journal of Psychiatry*, 173(11), 1094–1100. doi: 10.1176/appi.ajp.2016.15070854. Epub 2016 Aug 13. PMID: 27523496, PMCID: PMC5510596.

Glossary of Terms & Definitions

Ableism

Ableism is a term used to counter discrimination against people with disabilities based on the belief that typical abilities are superior.

Acceptable Use Policy (AUP)

A policy designed to limit how a computer or network can be used. Acceptable use policies (AUPs) usually include explicit statements about the required procedures, rights, and responsibilities of a technology user. Users are expected to acknowledge and agree to all AUP stipulations as a condition of system use.

Accessibility

Refers to the design of apps, devices, materials, and environments that support and enable access to content and educational activities for all learners. In addition to enabling students with disabilities to use content and participate in activities, the concepts also apply to accommodate the individual learning needs of students, such as English language learners, students in rural communities, or from economically disadvantaged homes. Technology can support accessibility through embedded assistance, for example, text-to-speech, audio and digital text formats of instructional materials, programs that differentiate instruction, adaptive testing, built-in accommodations, and assistive technology.

Adaptive Learning

Adaptive learning is an educational approach that uses technology and data analysis to tailor instruction and learning experiences to the individual needs of each student. It dynamically adjusts the content, difficulty level, and pace of learning based on real-time feedback and the student's performance. Adaptive learning is used in various educational settings, from K—12 to higher education and corporate training, to provide a more individualized and efficient learning experience.

Adaptive Lessons

These are educational activities that adjust in real time to meet the individual needs, skills, and learning pace of each student. These lessons use data and technology to modify content, difficulty levels, and instructional methods based on the student's performance and interactions.

Advocate

An advocate defends, supports, or promotes the cause or the interest of others.

Algorithm

A procedure used for solving a problem or performing a computation. Algorithms act as an exact list of instructions that conduct specified actions step by step in either hardware or software-based routines.[1]

Algorithm Bias

Algorithm bias describes systematic and repeatable errors in a computer system that create unfair outcomes, such as privileging one arbitrary group of users over others. It also occurs when an algorithm produces results that are systemically prejudiced due to erroneous assumptions in the machine learning process.[2]

Algorithmic Discrimination

Algorithmic discrimination occurs when automated systems contribute to unjustified/different treatment or impacts disfavoring people based on their race, color, ethnicity, sex (including pregnancy, childbirth, and related medical conditions, gender identity, intersex status, and sexual orientation), religion, age, national origin, disability, veteran status, genetic information, or any other classification protected by law. Depending on the specific circumstances, such algorithmic discrimination may violate legal protections.[3]

Algorithmic Literacy

The ability to understand how algorithms work, how they influence decision-making, and how they impact the information and services we interact with. It includes recognizing the biases or limitations of algorithms, understanding their role in digital systems, and knowing how they shape online experiences and outcomes.

Artificial Intelligence

A machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments.[4]

Artificial Intelligence in Education

Refers to the use of artificial intelligence technologies to enhance the educational process. This can include a variety of applications and tools designed to improve learning outcomes, support teachers, and personalize education for students.

Artificial Intelligence (AI) Literacy

#1 A set of competencies that enables individuals to critically evaluate artificial intelligence (AI) technologies; communicate and collaborate effectively with AI; and use AI as a tool online, at home, and in the workplace.[5]

#2 The ability to use, monitor, and critically evaluate AI output. AI literacy does not require the ability to create AI tools.[6]

#3 The skills associated with the ability to comprehend the basic principles, concepts, and applications of artificial intelligence, as well as the implications, limitations, and ethical considerations associated with artificial intelligence.[7]

Authentic Learning Experiences

Experiences that place learners in the context of real-world experiences and challenges.

Autism

Having a developmental disability significantly affects verbal and nonverbal communication and social interaction, generally evident before age 3, that adversely affects educational performance. Other characteristics often associated with autism are engagement in repetitive activities and stereotyped movements, resistance to environmental change or change in daily routines, and unusual responses to sensory experiences. A child is not considered autistic if the child's educational performance is adversely affected primarily because of an emotional disturbance.

Behavior

A person's external reaction to their environment. All behavior, such as yelling, crying, running, or throwing something, can be observed and measured.

Belittlement

The use of online forums, apps, or doctored images to try to insult and spread fake rumors, gossip, or untruths about a person.

Biodiversity

Biological diversity in an environment is indicated by the number of different species of plants and animals.

Bioregion

An area whose limits are naturally defined by topographic and biological features (such as mountain ranges and ecosystems) and not political or religious boundaries.

Blended Learning

In a blended learning environment, learning occurs online and in person augmenting and supporting teacher practice. Blended learning often allows students to have some control over the time, place, path, or pace of learning. In many blended learning models, students spend some of their face-to-face time with the teacher in a large group, some face-to-face time with a teacher or tutor in a small group, and some time learning with and from peers. Blended learning often benefits from a reconfiguration of the physical learning space to facilitate learning activities, providing a variety of technology-enabled learning zones optimized for collaboration, informal learning, and individual-focused study.

Child Predator

See Predator.

Child Sexual Exploitation and Abuse

Refers to the exploitation and abuse of children for sexual purposes. This can encompass a range of harmful behaviors, including but not limited to the following:

Sexual abuse: Engaging in sexual activities with a child, including molestation and rape.

Sexual exploitation: Using a child for sexual purposes, such as creating, distributing, or possessing child pornography or engaging in sexual trafficking.

Sexual grooming: The process of establishing an emotional connection with a child to gain their trust for sexual abuse or exploitation.[8]

Clickbait

Refers to sensationalized or misleading headlines and thumbnails used on Internet articles and videos designed to attract attention and encourage visitors to click on a link to a particular web page, with little regard to accuracy. Clickbait often promises more exciting content than it delivers.

Cognitive Development

The process of learning, memory, attention, concentration, and language development.

Cohesiveness

The degree to which group members enjoy collaborating with the other members of the group and are motivated to stay in the group.

Computer Type

According to storage and computing capacity, the classification of a computer is as follows: the number of users that it can support, the variety of input and output options it offers, and its physical size. Three major types of computers are mainframe computers, minicomputers, and personal computers (i.e., microcomputers).

Conformity

Adjusting one's behavior to align with the norms of a particular group.

Continuous Professional Education

Continous professional education (CPD) is how members of professions maintain, improve, and broaden their knowledge and skills and develop the personal qualities required in their professional lives, usually through a range of short and long training programs, some of which have an option of accreditation. This job-related continuing education and training refers to all organized, systematic education, and training activities in which people take part to obtain knowledge and/or learn new skills for a current or a future job, to increase earnings, to improve job and/or career opportunities in a current or another field, and to improve their opportunities for advancement and promotion. CPD activity is not part of the regular teaching activities supported through the institution's general grants and tuition fees paid by students enrolled in degree programs.[9]

Conspiracy Theory

An unfounded or poorly substantiated explanation of an event or situation, often blaming covert, powerful forces or entities without credible evidence.

Control of Institutions

A classification of institutions of elementary/secondary or postsecondary education by whether the institution is operated by publicly elected or appointed officials and derives its primary support from public funds (public control) or is operated by privately elected or appointed officials and derives its major source of funds from private sources (private control).

Counterfactual

Contrary to facts or thinking about alternative possibilities for past or future events: What might happen/have happened if…?

Critical thinking

The act or practice of thinking by applying reason and questioning assumptions to solve problems and evaluate information without the influence of biases, personal feelings, and opinions.

Crosscutting Concepts

Ideas that hold true across many and often disparate disciplines.

Customizing Learning

Also known as personalized learning, this is an educational approach that tailors instruction, content, and assessment to meet the individual needs, preferences, and abilities of each student. This method leverages data and technology to create a personalized educational experience that enhances student engagement and achievement.

Cyberbullying

Bullying is unwanted, aggressive behavior that involves a real or perceived power imbalance. This power imbalance can be physical. It can also revolve around popularity or the bully having access to embarrassing information about the victim. Generally, bullying is a repeated behavior or it has the potential to be repeated. Cyberbullying is when bullying behaviors occur online, either through messaging, social media, or other digital channels.[10]

Cyberspace

The digital environment is created by interconnected networks of information technology devices, including computers, servers, and the Internet.

Cyberstalking

This highly intimidating form of cyberbullying is when a person tracks another in the digital sphere and sends them negative comments, which can include threats, to frighten and terrorize them. In some cases, this can even lead to physical stalking in real life.[11]

Data Literacy

The ability to read, understand, interpret, and use data effectively. It involves knowing how to collect, analyze, and communicate insights from data to make informed decisions. Data literacy also includes understanding data sources, recognizing biases, and ensuring ethical handling of data.

Data Point

A discrete unit of information.

Dataset

Related data points in a collection, usually with tags (labels) and a uniform order.

Deforestation

The act of thinning or clearing of forests.

Deepfakes

Realistic but artificial media (typically video or audio) that is created using advanced AI techniques, designed to mimic real people and mislead viewers.

Deep Learning

A type of machine learning that can process a wider range of data resources (images, for instance), requires less human intervention, and can often produce more accurate results than traditional machine learning. Deep learning uses neural networks to ingest data and process it through multiple iterations that learn increasingly complex features of the data.[12]

Digital Citizen

Refers to an individual who engages responsibly, ethically, and positively in the digital world. Being a digital citizen involves using technology, especially the Internet, in a manner that respects the rights and well-being of others, while also contributing to the overall betterment of the online community. Digital citizenship encompasses a range of skills, knowledge, and attitudes that empower individuals to navigate the digital landscape safely and effectively. This includes understanding and practicing concepts such as online etiquette, responsible use of information, digital literacy, and awareness of potential risks and challenges in the digital environment.

Digital Citizenship

The safe, ethical, responsible, and informed use of technology. This concept encompasses a range of skills and literacies that can include Internet safety, privacy and security, cyberbullying, online reputation management, communication skills, information literacy, and creative credit and copyright.

The ability to use digital technology and media in safe, responsible, and ethical ways. Digital citizenship is a set of fundamental digital life skills that everyone needs to have.

Digital Civics

The study of the rights and responsibilities of citizens who inhabit the infosphere and access the world digitally.[13]

Digital Competence

Digital competence can be broadly defined as the confident, critical, and creative use of Information & Communication Technology to achieve goals related to work, employability, learning, leisure, inclusion, and/or participation in society.[14]

Digital Competitiveness

The ability to solve global challenges, innovate, and create new opportunities in the digital economy by driving entrepreneurship, jobs, growth, and impact.

Digital Content

Any type of content that exists in the form of digital data that are encoded in a machine-readable format, and can be created, viewed, distributed, modified, and stored using digital technologies. Examples of digital content include web pages and websites, social media, data and databases, digital audio, such as mp3s, e-books, digital imagery, digital video, video games, computer programs, and software.[15]

Digital Creativity

The ability to become a part of the digital ecosystem, and to create new knowledge, technologies, and content to turn ideas into reality.

Digital Decay

The gradual degradation or loss of digital content, data, or software over time due to technological obsolescence, data corruption, or the discontinuation of platforms or formats, all leading to challenges in accessing or preserving the information.

Digital Intelligence (DQ)

A comprehensive set of technical, cognitive, meta-cognitive, and socio-emotional competencies grounded in universal moral values that enable individuals to face the challenges of digital life and adapt to its demands. Thus, individuals equipped with DQ become wise, competent, and future-ready digital citizens who successfully use, control, and create technology to enhance humanity.[16]

Digital Literacy

The ability to use information and communication technologies to find, evaluate, create, and communicate information, which requires both cognitive and technical skills.[17]

Digital Natives

Young people who have been born into a virtual reality, view the world differently, and have a "digital footprint," process infographics speedily, but lack basic capacity for interpersonal interactions.

Digital Stewardship

Encompasses all activities related to the care and management of digital objects over time. Proper digital stewardship addresses all phases of the digital object lifecycle: from digital asset conception, creation, appraisal, description, and preservation, to accessibility, reuse, and beyond.[18]

Digital Use Divide

Traditionally, the digital divide referred to the gap between students who had access to the Internet and devices at school and home and those who did not. Significant progress is being made to increase Internet access in schools, libraries, and homes across the country. However, a digital use divide separates many students who use technology in ways that transform their learning from those who use the tools to complete the same activities but now with an electronic device (e.g., digital worksheets and online multiple-choice tests). The digital use divide is present in both formal and informal learning settings and across high- and low-poverty schools and communities.[19]

Disabilities, Children with

Those children evaluated as having any of the following impairments and who, by reason thereof, receive special education and related services under the Individuals with Disabilities Education Act (IDEA) according to an Individualized Education Program (IEP), Individualized Family Service Plan (IFSP), or a services plan. There are local variations in the determination of disability conditions, and not all states use all reporting categories.

Deaf-Blindness

Having concomitant hearing and visual impairments that cause such severe communication and other developmental and educational problems that the student cannot be accommodated in special education programs solely for deaf or blind students.

Developmental Delay

Having developmental delays, as defined at the state level and as measured by appropriate diagnostic instruments and procedures in one or more of the following cognitive areas: physical development, cognitive development, communication development, social or emotional development, or adaptive development. Applies only to 3- through 9-year-old children.

Disability

Term for impairments, activity limitations, and participation restrictions.

Dissing

When someone spreads false or negative information about a person, it damages their reputation.

Dogpiling

A term for a group response to a single post with an overwhelming amount of negativism and hate.

Doxing or Doxxing

Doxing is derived from the term “dropping dox” or “documents.” Doxing is a form of cyberbullying that uses sensitive or secret information, statements, or records for harassment, exposure, financial harm, or other exploitation of targeted individuals. It involves taking specific information about someone and then spreading it around the Internet or via some other means of getting it out to the public.[20]

Educator

The term is used to generically refer to any person involved in the process of teaching or transmitting knowledge. In particular, it refers to teachers at all levels of formal education, ranging from preprimary, primary, and secondary, to further and higher education (e.g. university lecturers), to vocational and adult education, and including initial training and continuous professional development. It may, by analogy, also be used to describe people involved in providing training in nonformal and informal settings, e.g., social workers, library staff, parents providing home schooling, etc.[21]

Elementary School

A school that offers more kindergarten through grade 4 than grades 5–8 and no grades 9–12.

Emotional Disturbance

Exhibiting one or more of the following characteristics over a long period, to a marked degree, and adversely affecting educational performance: an inability to learn that cannot be explained by intellectual, sensory, or health factors; an inability to build or maintain satisfactory interpersonal relationships with peers and teachers; inappropriate types of behavior or feelings under normal circumstances; a general pervasive mood of unhappiness or depression; or a tendency to develop physical symptoms or fears associated with personal or school problems. This term does not include socially maladjusted children unless they also display one or more of the listed characteristics.

Emotional Regulation

An individual's ability to manage and respond to emotional experiences such as stress, anxiety, mood, temperament, and hyperactivity/impulsivity.

Empathy

To understand, be aware, and be sensitive to the experiences feelings, and thoughts of another person.

Encryption

The process of translating a file into an unintelligible format (i.e., to encode it) via the use of mathematic algorithms or other encoding mechanisms. In general terms, the recipient of an encrypted message must possess a matching key to decrypt and read the message.

Energetic Play

Active play is equivalent to moderate-to-vigorous physical activity when children get out of breath and feel warm. This may take many forms and may involve other children, caregivers, objects, or not.

Ethics

Ethics are an external social system relating to a specific group that defines right and wrong behaviors. They are codified into a set of rules or a system and adopted by people in that field. Ethical principles remain consistent across industries and institutions, as they offer strict behavior guidelines.[22]

Equity

In education, equity means increasing all student's access to educational opportunities with a focus on closing achievement gaps and removing barriers that students face based on their race, ethnicity, or national origin; sex; sexual orientation or gender identity or expression; disability; English language ability; religion; socioeconomic status; or geographical location.

Executive Function

Executive function is an imposing name for a group of essential mental tasks, including planning, strategizing, organizing, setting goals, and paying attention to the important details, that will help to achieve those goals.[23]

Fake News

This is information whose content is deliberately fabricated or manipulated and presented as real news, with the intent to deceive or misinform the public.

Fake News Creators

These are entities responsible for conceiving, writing, and disseminating fake news. This can include the owners and operators of sites that publish fake news stories and affiliated social media accounts, as well as the manufacturers of the fake news stories — whether they are publicly identified or remain anonymous.[24]

Fake News Purveyors

These are websites, social media pages, and accounts, or individuals who share or aggregate fake news stories. Purveyors may attempt to spread fake news stories on purpose, and unknowing purveyors may share fake news without realizing it is fake.[25]

Flaming

When extreme or offensive language is used to try and cause stress or anxiety to the victim.

Fraping

When someone pretends to be someone else online and posts something silly or inappropriate. It can be intended as a joke, but in some cases, it can cause serious negative repercussions.

Gamers

Gamers are people who play video games.

Gaming

Gaming is playing an electronic video game, which is often done on a gaming console, PC, smartphone, or another electronic device.

Gaslighting

It happens when someone is manipulated to question if their recollection of events or activities happened the way they remember it.

Generative Artificial Intelligence (genAI) Literacy

Refers to the knowledge and skills required to understand, effectively use, and critically evaluate genAI systems. This includes the ability to comprehend how genAI models, such as those used in text, image, or code generation; function;

the ethical implications of their use; and the potential biases and limitations inherent in these technologies. genAI literacy enables individuals to interact with AI-generated content responsibly, make informed decisions about its applications, and contribute to discussions about the societal impact of generative AI.

Gender Identity

One's inner sense of one's gender, which may or may not match the sex assigned at birth.

Generation Alpha

Refers to the cohort of people born from the early 2010s to 2025. This generation follows Generation Z and is typically characterized by being highly tech-savvy and immersed in digital environments from a young age. This generation is also referred to as "honey badger" due to their fierce nature and independent approach.

Generation Beta or Gen Beta

Refers to the cohort of people born from 2025 to 2039. This generation follows Generation Alpha.

Generative Artificial Intelligence

Refers to deep learning models that can generate high-quality text, images, and other content based on the data they were trained on; generative models can take raw data and "learn" to generate statistically probable outputs when prompted.[26]

Grooming (a.k.a. Cyber Grooming)

The process of "befriending" a young person online to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse.

Hacking

Refers to the process of exploiting weaknesses in a computer system, network, or software application to gain unauthorized access or cause damage. It encompasses a broad range of activities, some of which can be legal and ethical (white-hat hacking), while others are illegal and malicious (black-hat hacking).

Harassment

Constant online abuse can occur on messaging apps or via comments on social media sites, chat rooms, or gaming sites. Conduct that is unwelcome and denies or limits a student's ability to participate in or benefit from a school's education program. The conduct can be verbal, nonverbal, or physical and can take many forms, including verbal acts and name-calling, as well as nonverbal conduct, such as graphic and written statements, or conduct that is physically threatening, harmful, or humiliating.

Hearing Impairment

Having a hearing impairment, whether permanent or fluctuating, which adversely affects the student's educational performance, is not included under the definition of "deaf" in this section.

High-Level Machine Intelligence

Refers to a form of artificial intelligence that can perform most tasks that are economically relevant and require human intelligence, at or above the level of an average human. **High-level machine intelligence** (HLMI) would be capable of autonomously solving complex problems across a wide range of domains, potentially matching or exceeding human performance in tasks such as reasoning, decision-making, language understanding, and perception.

Homeschool Students

Students are considered to be homeschooled if all of the following conditions are met: Their parents reported them being schooled at home instead of at a public or private school, their enrollment in public or private schools did not exceed 24 hours a week (or 25 hours a week before 2019), and they were not being homeschooled only due to a temporary illness. Homeschooled students include those ages 5–17 with a grade equivalent of kindergarten through grade 12.

Honey Badger

See "Generation Alpha".

Human–Computer Interaction

A multidisciplinary field of study focusing on the design of computer technology and, in particular, the interaction between humans (the users) and computers.[27]

Hyperpartisan Websites

These are websites that promote extreme political biases, often skewing facts to serve a specific ideological agenda.

Identity Theft

When a cybercriminal steals someone's personal information and uses it to assume their identity. This can involve the criminal applying for credit and loans, or even filing taxes using the victim's identity, potentially damaging their credit status.

Identity Politics

Coined by Jonathan Rauch of The Brookings Institution, it is the political mobilization organized around group characteristics such as race, gender, sexuality and not around party, ideology, or monetary ideals. It is not new, illegitimate, or nefarious.[28]

Information Disorder

A broad term that encompasses all types of problematic information, including misinformation, disinformation, and malinformation, which cause confusion or harm.

Information Literacy

Students receive scaffolding and support for research processes as they access, locate, curate, and evaluate information content, using library databases and the open Internet to appreciate how expertise and authority are constructed and contextual.[29]

Information Steward

An individual with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

Individuals with Disabilities Education Act (IDEA)

A federal law was enacted in 1990 and reauthorized in 1997 and 2004. IDEA requires services for children with disabilities throughout the nation. IDEA governs how states and public agencies provide early intervention, special education, and related services to eligible infants, toddlers, children, and youth with disabilities. Infants and toddlers with disabilities (birth to age 2) and their families receive early intervention services under IDEA, Part C. Children and youth (ages 3–21) receive special education and related services under IDEA, Part B.

Individualized Learning

An educational approach that tailors instruction to meet the unique needs, strengths, interests, and learning pace of each student. This method aims to provide customized educational experiences that enhance student engagement and achievement by addressing individual differences in learning styles and abilities. Individualized learning leverages various tools and technologies, including adaptive learning software, to effectively support diverse learners and foster a more inclusive educational environment.

Intellectual Disability

Having significantly subaverage general intellectual functioning, existing concurrently with defects in adaptive behavior and manifested during the developmental period, which adversely affects the child's educational performance.

Internet Safety

Internet safety or "e-safety" includes knowing about one's Internet privacy and how one's behaviors can support a healthy interaction with the use of the Internet.[30]

Impersonation

Creating a fake social media account or email address to pretend to be someone else and then using it for negative purposes.

Interactive Lessons

Are educational activities designed to engage students actively in the learning process through the use of technology, hands-on activities, and participatory techniques. These lessons involve direct interaction between the student and the learning materials, often incorporating multimedia elements, simulations, and real-time feedback to enhance understanding and retention.

Intimidation

Placing another person in reasonable fear of bodily harm through the use of threatening words and/or other conduct, but without displaying a weapon or subjecting the victim to actual physical attack.

Large Language Models

Large Language Models (LLMs) are deep learning algorithms that can recognize, summarize, translate, predict, and generate content using very large datasets.[31]

Machine Learning

A subcategory of artificial intelligence, in which the study or the application of computer algorithms is designed to improve automatically through experience. Machine learning (ML) algorithms build a model based on training data to perform a specific task, like aiding in prediction or decision-making processes, without necessarily being explicitly programmed to do so.

Malinformation

This is information that is based on reality but is used with harmful intent, often by revealing private, sensitive, or true information to deliberately cause harm, manipulate public perception, or damage reputations. It differs from misinformation (false but not intended to harm) and disinformation (deliberately false with intent to mislead).

Malware (short for malicious software)

Is a type of software designed to harm, exploit, or otherwise compromise the operation of computers, networks, or devices.

Masquerading

See Impersonation

Mean Girl Behavior

Is a type of behavior where girls engage in hostility toward their peers. This can take many forms, including excluding others from social activities, publicly criticizing or belittling others, and spreading rumors.

Media Literacy

The ability to use information and communication technologies to find, evaluate, create, and communicate information, requires both cognitive and technical skills. Students who are media literate are equipped with the skills to recognize when information is needed and have the ability to locate, evaluate, and use the information effectively.[32]

Mentor

A role model for the child. Offers encouragement and support, and the child trusts the mentor to assist them with difficult situations or concepts.

Metabolic Equivalent of Task (MET)

The metabolic equivalent of task, or simply metabolic equivalent, is a physiological measure expressing the energy cost (or calories) of physical activities. One MET is the energy equivalent expended by an individual while seated at rest.

Middle School

A school that offers more grades 5 through 8 than higher or lower grades but does not offer both kindergarten through grade 4 and grades 9 through 12.

Misleading Information

Information that may not be outright false but is manipulated, taken out of context, or selectively presented to mislead the audience.

Multiple Disabilities

Having concomitant impairments (such as intellectually disabled-blind and intellectually disabled-orthopedically impaired), the combination of which causes such severe educational problems that the student cannot be accommodated in special education programs solely for one of the impairments. The term does not include deaf-blind students.

Multi-Tiered System of Supports (MTSS)

A proactive and preventative framework that integrates data and instruction to maximize student achievement and support students' social, emotional, and behavioral needs from a strengths-based perspective.[33]

Negging

The act of insulting, deriding, or otherwise putting down an individual or group by another in an attempt to shake, crack, and eventually crumble their inherent confidence.[34]

Neural Network

Also known as an artificial neural network, neural net, or deep neural net; a computer system inspired by living brains.

Neuroscience

Examines the structure and function of the human brain and nervous system. The study of neuroscience in education and learning is rapidly developing.

News Literacy

Driven by rising interest in "fake news" and disinformation, students learn to understand, interpret, and evaluate different forms of news, analysis, and opinion.[35]

Nonconsensual Explicit Imagery (NCEI)

Refers to the distribution or sharing of sexually explicit images or videos of an individual without their consent. This typically involves private or intimate content that was originally created with the understanding that it would remain confidential. The unauthorized dissemination of such material often occurs online or via digital means and can lead to severe emotional, psychological, and reputational harm to the individual depicted. NCEI is considered a serious violation of privacy and is illegal in many State, Federal, and Provincial jurisdictions.

Nonconsensual Pornography

The sharing or distribution of sexually explicit images or videos of someone without their consent. This often involves intimate images that were shared privately but later distributed without permission and can lead to legal consequences under various privacy and cyber laws. May also be known as "revenge porn."

Non-screen-based Sedentary Time

Usually refers to time spent sitting, not using screen-based entertainment. For young children, this includes lying on a mat; sitting in a highchair, pram, or stroller with little movement; sitting reading a book; or playing a sedate game.

Norms

The acceptable standards of behavior within a group, are shared by the members.

Online Learning

Also known as e-learning or digital learning, is a method of education where instruction and content delivery occur over the Internet. It allows students to access educational materials, participate in courses, and interact with instructors and peers remotely, often through various digital platforms and tools. Online learning is widely used in various educational contexts, including K—12 education, higher education, professional development, and corporate training, providing flexible and scalable learning opportunities.

Online Recruiter

The process of "befriending" a young person online to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse.

Openly Licensed Educational Resources

Teaching, learning, and research resources that reside in the public domain or have been released under a license that permits their use, modification, and sharing with others. Open resources may be full online courses, digital textbooks, or more granular resources such as images, videos, and assessment items.

Open-Source Intelligence

Techniques involve the collection and analysis of publicly available information from various sources, such as websites, social media, forums, and databases, to gather actionable insights. These techniques are used in fields like cybersecurity, law enforcement, and competitive analysis to assess threats, trends, or individual profiles without the need for covert methods.

Organization for Economic Cooperation and Development (OECD)

An intergovernmental organization of industrialized countries that serves as a forum for member countries to cooperate in research and policy development on social and economic topics of common interest. In addition to member countries, partner countries contribute to the OECD's work in a sustained and comprehensive manner.

Orthopedic Impairment

Having a severe orthopedic impairment that adversely affects a student's educational performance. The term includes impairment resulting from congenital anomaly, disease, or other causes.

Other Health Impairments

Having limited strength, vitality, or alertness due to chronic or acute health problems, such as a heart condition, tuberculosis, rheumatic fever, nephritis, asthma, sickle cell anemia, hemophilia, epilepsy, lead poisoning, leukemia, or diabetes, which adversely affect the student's educational performance.

Outcomes

Something that follows as a result or consequence, a conclusion reached through a process of logical thinking.

Outing

See Trickery

Password

A confidential and alphanumeric sequence of characters that serves as a form of authentication, allowing an individual to access a computer system, online account, or digital device. The user must provide the correct password, which is known only to them, to verify their identity and gain authorized entry. Passwords play a crucial role in securing digital information and preventing unauthorized access to personal or sensitive data.

Password Hygiene

Creating unique and separate passwords for sensitive online accounts, managing passwords using browser or stand-alone applications, and the tactics of changing passwords.

Passphrase

A sequence of words or other text used as a form of authentication to access a computer system, online account, or digital device. Unlike traditional passwords, passphrases are typically longer and consist of multiple words or a combination of words, numbers, and symbols. Passphrases enhance security by creating a more complex authentication mechanism, making it harder for unauthorized individuals or automated programs to guess or crack access credentials.

Peer Influence

Peer influence is **choosing to do something you wouldn't otherwise do** because you want to feel accepted and valued by your friends.

Peer Pressure

Peer pressure is doing something because you want to feel accepted and valued by your friends.

Peer Susceptibility

Peer susceptibility is the likelihood that conformity will occur when exposed to peer pressure/peer influence.

Personalized Learning

Refers to instruction in which the pace of learning and the instructional approach are optimized for the needs of each learner. Learning objectives, instructional approaches, and instructional content (and its sequencing) may all vary based on learner needs. In addition, learning activities are meaningful and relevant to learners, driven by their interests, and often self-initiated.

Pervasive Computing

Also known as ubiquitous computing, refers to the integration of computing technology into everyday objects and environments, making them smart, connected, and capable of interacting with each other and with users seamlessly. The goal of pervasive computing is to create an environment where computational power is embedded in the fabric of daily life, making it unobtrusive and enhancing user experiences.

Pervasive Education

Typically refers to the integration and widespread presence of educational technologies, digital tools, and learning opportunities throughout various aspects of a learner's life and environment. It encompasses the idea that education is not confined to traditional classroom settings but extends into the broader context of a learner's daily experiences.

Pervasive Technology

Refers to the widespread integration and seamless presence of technology in various aspects of daily life and across diverse environments. In a pervasive technology landscape, digital tools, devices, and systems become an integral and often unnoticed part of the fabric of society, enhancing and influencing the way people live, work, and interact.

Phishing

A cyberattack technique in which attackers impersonate a trusted entity to deceive individuals into providing sensitive information, such as usernames, passwords, or financial details. This is typically done through fraudulent emails, messages, or websites that appear legitimate.

Pig Butchering Scam

A sophisticated type of online fraud where scammers build a long-term, fake relationship with the victim (the "pig") before conning them into investing in a fraudulent scheme. Once the victim has invested a significant amount of money, the scammers "butcher" the relationship by disappearing with the funds, leaving the victim with major financial losses.

Positive Behavioral Interventions and Supports (PBIS)

A framework for creating safe, positive, equitable schools, where every student can feel valued, connected to the school community, and supported by caring adults.[36]

Predator

A predator is a person who looks for other people to use, control, or harm them in some way.

Prekindergarten

Preprimary education for children typically ages 3–4 who have not yet entered kindergarten. It may offer a program of general education or special education and may be part of a collaborative effort with Head Start.

Preschool

An instructional program enrolling children generally younger than 5 years of age and organized to provide children with educational experiences under professionally qualified teachers during the year or years immediately preceding kindergarten (or before entry into elementary school when there is no kindergarten).

Project-based Learning

Takes place in the context of authentic problems, continues over time, and brings in knowledge from many subjects. Project-based learning, if properly implemented and supported, helps students develop 21st-century skills including creativity, collaboration, and leadership, and engages them in complex, real-world challenges that help them meet expectations for critical thinking.

Propaganda

This is information that is often biased or misleading, that is disseminated to influence public opinion or promote a political agenda.

Public Charter School

A school providing free public elementary and/or secondary education to eligible students under a specific charter granted by the state legislature or other authority and designated by such authority to be a charter school.

Psycho-education

Intervention for patients and family/guardian that provides information and support to better understand and cope with illness.

Quishing

A form of phishing that uses QR codes as the delivery mechanism for fraudulent websites or malware, tricking users into scanning the codes, which can lead to credential theft or device compromise.

Responsible AI and Tech Justice

A robust and comprehensive course of study that utilizes an explicit racial and social justice lens to equip all students with the knowledge and resources to critically interrogate the ethical and equitable development, deployment, and impacts of AI, while simultaneously challenging, disrupting, and remedying the harms that these various technologies can cause within individual's lives, communities, and society at large.[37]

Repurpose

The use of something for a purpose other than its original intended use, or the purpose for which it has been currently used.

Response to Intervention (RTI)

A data-driven approach schools use to support students academically. This approach is characterized by analyzing assessment data, planning high-quality instruction, implementing interventions, and evaluating each student's RTI.[38]

Revenge Porn

The illegal activity of posting nonconsensual pornography without consent.

Risk

In information and technology security, risk refers to the potential for loss or harm resulting from a threat exploiting a vulnerability in a system, process, or asset. It is typically measured by considering the likelihood of a threat occurring and the potential impact on the organization's data, infrastructure, or operations. Risk involves the intersection of threats, vulnerabilities, and the value of the impacted assets.

Risk Assessment

In information and technology security, risk assessment is the process of identifying, evaluating, and prioritizing potential risks to an organization's information systems and data. It involves analyzing threats, vulnerabilities, and the potential impact of security incidents to determine the likelihood and severity of risks. The goal is to provide a clear understanding of risks so that informed decisions can be made to mitigate or manage them effectively.

Risk Management

In information and technology security, risk management is the process of identifying, assessing, prioritizing, and mitigating risks to an organization's information systems and assets. It involves implementing strategies and controls to reduce the likelihood and impact of threats exploiting vulnerabilities, ensuring the protection of critical data and resources while aligning with the organization's overall objectives. Risk management seeks to balance security efforts with operational needs and cost-effectiveness.

Role

A set of expected behavior patterns attributed to someone occupying a given position in a social unit.

Satire

A form of comedic or exaggerated content that mimics real news but with no intention to deceive used to mock or criticize societal and political issues.

Science, Technology, Engineering, and Mathematics (STEM)

Fields of study that are considered to be of particular relevance to advanced societies. For the Condition of Education, STEM fields include biological and biomedical sciences, computer and information sciences, engineering and engineering technologies, mathematics and statistics, and physical sciences and science technologies. STEM occupations include computer scientists and mathematicians; engineers and architects; life, physical, and social scientists; medical professionals; and managers of STEM activities.

Screen Time

Refers to the time an individual spends using electronic or digital media devices such as televisions, smartphones, tablets, or computers.[39]

Secondary/High School

A school that offers more grades 9 through 12 than grades 5 through 8 and no kindergarten through grade 4.

Sedentary Screen Time

Time spent passively watching screen-based entertainment (TV, computer, mobile devices). Does not include active screen-based games where physical activity or movement is required.

Self-assessment

Involves the ability to be a realistic judge of one's performance. Proponents of self-assessment suggest it has many advantages; for example, it provides timely and effective feedback and allows students to assess their learning quickly; allows instructors to understand and provide quick feedback on learning; promotes academic integrity through student self-reporting of learning progress; promotes the skills of reflective practice and self-monitoring; develops self-regulated learning; increases student motivation; improves satisfaction from participating in a collaborative learning environment; and helps students develop a range of personal, transferrable skills to meet the expectations of future employers.[40]

Self-assessment Tool

A self-assessment tool is an instrument that assists professionals in their self-assessment, i.e., in evaluating the effectiveness of their performance in all areas of responsibility, and determining what improvements are required. Self-assessment tools may be found in online programs in the form of questionnaires which allow teachers to evaluate their digital competence with the help of a set of questions. Usually, feedback in the form of a report is provided, identifying areas of strength and areas for development.[41]

Self-determined Learning

A process in which learners take the initiative to identify learning needs, formulate learning goals, identify learning resources, implement problem-solving strategies, and reflect upon the learning processes to challenge existing assumptions and increase learning capabilities.[42]

Self-directed Learning

A process in which learners take responsibility, typically under the guidance of an instructor, for diagnosing learning needs, articulating learning goals, identifying materials and resources for learning, choosing and implementing appropriate learning strategies, and evaluating learning outcomes.[43]

Self-regulated Learning

Refers to learning that is guided by metacognition (thinking about one's thinking), strategic action (planning, monitoring, and evaluating personal progress against a standard), and motivation to learn. "Self-regulated" describes a process of taking control of and evaluating one's learning and behavior. The concept is related to the concepts of self-directed and self-determined learning.[44]

Sexting

The act of sending, receiving, or forwarding sexually explicit messages, photographs, or videos, primarily between mobile phones, but also through any digital messaging system. This often involves personal content that is intended to remain private between individuals.

Sextortion

The threatened dissemination of explicit, intimate, or embarrassing images of a sexual nature without consent, usually to procure additional images, sexual acts, money, or something else.[45] When a sexual predator coerces the child (or adult) to send sexually explicit images of themselves and once received threatens to expose the images unless certain demands are met. Often the demand is for more explicit images, money, or to meet in person.

Sexts

Sexually explicit messages, photographs, or videos are sent and received primarily through mobile phones, but also via other digital messaging systems. This form of communication often involves personal content intended to remain private between individuals. However, sexting can carry significant risks, including privacy violations, emotional distress, and legal consequences, especially when involving minors. It is important for individuals to be aware of the potential implications and to handle such content with extreme caution.

Sexual Predator

A sexual predator is a person who commits sexual crimes against other people.

SMiShing

A phishing attack is conducted via SMS (short message service), where attackers send fraudulent messages to trick individuals into revealing personal information, and credentials, or installing malicious software on their mobile devices.

Shallowfakes

A term used to describe videos or images that are altered using basic editing tools (such as cropping, slowing down, or speeding up footage) rather than advanced AI techniques used in creating deepfakes. These manipulations are often subtle but can still mislead viewers by presenting a distorted version of reality without the complexity of deep neural networks used to create deepfakes.

Social and Emotional Learning

A strengths-based, developmental process that begins at birth and evolves across the lifespan. The process through which children, adolescents, and adults learn skills to support healthy development and relationships.

Social Media

Refers to websites and applications designed to allow people to share content quickly, efficiently, and in real time. Most social media platforms enable users to create and share content or to participate in social networking. They often include features like profile creation, content sharing, messaging, and the ability to connect with others through friend requests or follows. Examples of popular social media platforms include Facebook, Twitter, Instagram, and TikTok. These platforms are used for a variety of purposes including personal expression, information dissemination, marketing, and community building.

Social Networking

Refers to the use of Internet-based platforms that allow individuals to interact with each other, share information, and create online communities. These platforms provide users with various ways to communicate, such as through posts, comments, instant messaging, and media sharing. Examples include sites like Facebook, Instagram, Twitter, and LinkedIn. Social networking sites can be used for both personal interaction and professional networking.

Social Responsibility of AI

Refers to a human value-driven process where values such as Fairness, Transparency, Accountability, Reliability, Safety, Privacy and Security, and Inclusiveness are the principles; designing Socially Responsible AI Algorithms is the means; and addressing the social expectations of generating shared value — enhancing both AI's ability and benefits to society — is the main objective.[46]

Spear Phishing

A targeted phishing attack is aimed at a specific individual or organization, where attackers gather detailed personal information to craft highly convincing fraudulent emails to steal sensitive data or user credentials.

Specific Learning Disability

Having a disorder in one or more of the basic psychological processes involved in understanding or in using spoken or written language, may manifest itself in an imperfect ability to listen, think, speak, read, write, spell, or do mathematical calculations. The term includes such conditions as perceptual disabilities, brain injury, minimal brain dysfunction, dyslexia, and developmental aphasia. The term does not include children who have learning problems that are primarily the result of visual, hearing, motor, or intellectual disabilities, or of environmental, cultural, or economic disadvantage.

Speech or Language Impairment

Having a communication disorder, such as stuttering, impaired articulation, language impairment, or voice impairment, that adversely affects the student's educational performance.

Spoofing

Refers to the act of impersonating a legitimate entity to deceive or mislead individuals or systems. This can involve techniques such as falsifying email addresses, IP addresses, or other identifying information to gain unauthorized access, steal data, or distribute malware.

Traumatic Brain Injury

Having an acquired injury to the brain caused by an external physical force, resulting in total or partial functional disability psychosocial impairment or both, that adversely affects the student's educational performance. The term applies to open or closed head injuries resulting in impairments in one or more areas, such as cognition; language; memory; attention; reasoning; abstract thinking; judgment; problem-solving; sensory, perceptual, and motor abilities; psychosocial behavior; physical functions; information processing; and speech. The term does not apply to brain injuries that are congenital or degenerative, or to brain injuries induced by birth trauma.

Tribal Colleges and Universities

An institutional classification developed by the Andrew W. Carnegie Foundation for the Advancement of Teaching. Tribal colleges and universities, with few exceptions, are tribally controlled and located on reservations. They are all members of the American Indian Higher Education Consortium.

Trickery

When someone is groomed to build a relationship of trust and trick them into providing personal details or photos — they are then used to humiliate the person.

Trolling

Making constant comments to try and get a reaction out of the person. Some trolling can be intended as a harmless joke but often it has a malicious intent.

Trustworthy Artificial Intelligence

Artificial intelligence (AI) systems that exhibit characteristics like resilience, integrity, security, and privacy if they're going to be useful and people can adopt them without fear.[47]

Virtual Learning Environment

Is a web-based platform for the digital aspects of courses of study, usually within educational institutions. **Virtual Learning Environment** (VLEs) typically allow participants to be organized into cohorts, groups, and roles; present resources, activities, and interactions within a course structure; provide for the different stages of assessment; report on participation; and have some level of integration with other institutional systems.[48]

Virtue

A quality or trait deemed to be morally good, embodying standards of right behavior and ethical conduct. Virtues are principles that guide individuals in acting honorably and with integrity in various situations.

Visual Impairment

Having a visual impairment that, even with correction, adversely affects the student's educational performance. The term includes partially seeing and blind children.

Volunteer

To do something, especially for other people or for an organization, willingly and without being forced or paid to do it.[49]

Vulnerabilities

In the context of computer security, refers to weaknesses or flaws in software, hardware, or organizational processes that can be exploited by attackers to gain unauthorized access, disrupt operations, or steal sensitive information.

Vishing

Voice phishing is where attackers use phone calls or voice messages to impersonate legitimate entities (e.g., banks or government agencies) and trick victims into providing personal information or transferring money.

Whaling

A type of spear phishing attack that specifically targets high-profile individuals such as executives or decision-makers, often to obtain sensitive business information or initiate large financial transactions.

Bibliography

American Institutes for Research, 2023, “Essential Components of MTSS,” https://mtss4success.org/essential-components#:~:text=A%20multi%2Dtiered%20system%20of,from%20a%20strengths%2Dbased%20perspective.

Center on Positive Behavioral Interventions & Supports, 2023, “What Is PBIS?” www.pbis.org, www.pbis.org/pbis/what-is-pbis.

Interval Technology Partners, LLC, 2025, “RTI vs. MTSS,” National Center for Education Statistics (NCES), 2023, “Children’s Internet Access at Home. Condition of Education, Glossary,” U.S. Department of Education, Institute of Education Science, https://nces.ed.gov/programs/coe/indicator/cch, and https://nces.ed.gov/programs/coe/glossary#race.

NIST, January 21, 2020, “Trustworthy AI: A Q&A with NIST’s Chuck Romine,” www.nist.gov/blogs/taking-measure/trustworthy-ai-qa-nists-chuck-romine.

Some definitions came directly from these sources, while others were excerpted or adapted for clarity, brevity, and relevancy.

U.S. Department of Education, Office of Educational Technology, January 2017, “Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update,” Washington, D.C., Department of Education, http://tech.ed.gov.

Virgin Media, (n.d.), “How to introduce the kids to the Internet,” www.virginmedia.com/blog/online-safety/childrens-internet-safety-test.

World Health Organization, 2019, “Guidelines on Physical Activity, Sedentary Behaviour, And Sleep for Children Under 5 Years of Age,” ISBN 978-92-4-155053-6.

Notes

1 Gillis, A., “What Is an Algorithm?” Tech Target, www.techtarget.com/whatis/definition/algorithm.

2 Florida State University, 2024, “Algorithm Bias,” Florida State Libraries, https://guides.lib.fsu.edu/algorithm.

3 Office of Science and Technology Policy, June 2022, “White House OTSP AI Bill of Rights, Blueprint for an AI Bill of Rights,” https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

4 The White House, October 30, 2023, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

5 Long, D., & Magerko, B., 2020, "What Is AI Literacy? Competencies and Design Considerations," *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3313831.3376727, as appearing in Recommendations: Enhancing AI Literacy for the United States of America, National Artificial Intelligence Advisory Committee (NAIAC), November 2023, www.google.com/url?sa=i&url=https%3A%2F%2Fai.gov%2Fwp-content%2Fuploads%2F2023%2F12%2FRecommendations_Enhancing-Artificial-Intelligence-Literacy-for-the-United-States-of-America.pdf&psig=AOvVaw2EimGyfw1_dpqyNWRV-u0i&ust=1716838685518000&source=images&cd=vfe&opi=89978449&ved=0CAUQn5wMahcKEwjQhqPRiKyGAxUAAAAAHQAAAAAQBg.

6 Adapted from Long, D., & Magerko, B., 2020. "What Is AI Literacy? Competencies and Design Considerations," C*HI'20: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1–16. https://doi.org/10.1145/3313831.3376727, as appearing in Recommendations: Enhancing AI Literacy for the United States of America, National Artificial Intelligence Advisory Committee (NAIAC), November 2023, www.google.com/url?sa=i&url=https%3A%2F%2Fai.gov%2Fwp-content%2Fuploads%2F2023%2F12%2FRecommendations_Enhancing-Artificial-Intelligence-Literacy-for-the-United-States-of-America.pdf&psig=AOvVaw2EimGyfw1_dpqyNWRV-u0i&ust=1716838685518000&source=images&cd=vfe&opi=89978449&ved=0CAUQn5wMahcKEwjQhqPRiKyGAxUAAAAAHQAAAAAQBg.

7 The Artificial Intelligence (AI) Literacy Act, December 15, 2023, Rep. Lisa Blunt Rochester (D-DE) and Rep. Larry Bucshon (R-IN), www.google.com/url?sa=i&url=https%3A%2F%2Fbluntrochester.house.gov%2Fuploadedfiles%2F20231215_ai_text.pdf&psig=AOvVaw2EimGyfw1_dpqyNWRV-u0i&ust=1716838685518000&source=images&cd=vfe&opi=89978449&ved=0CAUQn5wMahcKEwjQhqPRiKyGAxUAAAAAHQAAAAAQBA.

8 World Health Organization, "Sexual Exploitation and Abuse," www.who.int/docs/default-source/documents/ethics/sexual-exploitation-and-abuse-pamphlet-en.pdf?sfvrsn=409b4d89_2.

9 Multirank, 2024, https://benchmarking.umultirank.org/, retrieved May 2024.

10 Karppinen, I., Nurse, J. R. C., & Varughese, J., 2023, "Oh Behave! The Annual Cybersecurity Attitudes and Behaviors Report 2023," The National Cybersecurity Alliance and CybSafe, www.cybsafe.com/whitepapers/cybersecurity-attitudes-and-behaviors-report.

11 Virgin Media, (n.d.), "How to Introduce the Kids to the Internet," www.virginmedia.com/blog/online-safety/childrens-internet-safety-test.

12 McKinsey & Company, April 3, 2024, "What Is AI (Artificial Intelligence)?" www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-ai.

13 Clements, E., 2010, "What Is Digital Civics," www.digitalcivics.org/what-is-digital-civics/.

14 Punie, Y., & Redecker, C., editor(s), 2017, "European Framework for the Digital Competence of Educators: DigCompEdu," EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 2024.

15 Punie, Y., & Redecker, C. editor(s), 2017, "European Framework for the Digital Competence of Educators: DigCompEdu," EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 2024.

16 Park, Y., 2019, “DQ Global Standards Report 2019,” Common Framework for Digital Literacy, Skills and Readiness, DQ Institute, https://www.dqinstitute.org/wp-content/uploads/2019/11/DQGlobalStandardsReport2019.pdf

17 American Library Association, 2024, “Digital Literacy, ALA’s Digital Literacy Task Force,” https://literacy.ala.org/digital-literacy/.

18 McCurry, J., April 2, 2014, “Digital Stewardship: The One with All the Definitions.” The Collation (blog), Folger Shakespeare Library, https://collation.folger.edu/2014/04/digital-stewardship-the-one-with-all-the-definitions, preserved at https://perma.cc/V77P-A24X.

19 U.S. Department of Education, January 2017, “Reimagining the Role of Technology in Education: 2017 National Education Technology Plan Update,” U.S. Department of Education, Office of Educational Technology, Washington, D.C., Department of Education, http://tech.ed.gov.

20 (n.a.) (n.d.), “Doxing Definition,” What Is Doxing? What Does It Mean to Dox Someone? | Fortinet, retrieved June 5, 2024.

21 Punie, Y., & Redecker, C., editor(s), 2017, “European Framework for the Digital Competence of Educators: DigCompEdu,” EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 2024.

22 Lederman, D., 2024, “Ethics versus Morals: A Comparison,” Center for Public Trust, https://thecpt.org/2023/03/24/ethics-versus-morals-a-comparison-2/.

23 Scholastic Parents Staff, (n.d.), “Explaining Executive Function,” Explaining Executive Function (scholastic.com), retrieved June 6, 2024.

24 Candace, B, May 6, 2025, “What is Fake News”? William & Mary Libraries. https://guides.libraries.wm.edu/fakenews

25 OU Libraries, August 12, 2024, “Fake News and Information Literacy,” Library of the University of Oregon, https://guides.libraries.wm.edu/fakenews, retrieved, September 19, 2024.

26 IBM, 2024, “What Is Generative AI?” IBM Corp., https://research.ibm.com/blog/what-is-generative-AI?utm_content=SRCWW&p1=Search&p4=43700078077908973&p5=e&gclid=CjwKCAiA75itBhA6EiwAkho9e2TEgZlNKf1pCAOCZrpjrj3Dcwo5U0uXL_JujfcBVHKwp85Iqx3ZxhoCIskQAvD_BwE&gclsrc=aw.ds.

27 Interaction Design Foundation, 2024, “What Is Human-Computer Interaction (HCI)?” www.interaction-design.org/literature/topics/human-computer-interaction.

28 Lukianoff, G., & Haidt, J., 2018, *The Coddling of the American Mind: How Good Intentions and Bad Ideas are Setting up a Generation for Failure*, pp. 59-60.

29 Hobbs, R., Chapman, D., Doerr-Stevens, C., et al., April 9, 2022, “Media Education in English Language Arts,” National Council of Teachers of English, https://ncte.org/statement/media_education, retrieved October 7, 2024.

30 Common Sense, 2020, “How Can I Keep My Private Data Safe and Secure?” www.commonsense.org/education/digital-citizenship/topic/privacy-and-security, retrieved June 19, 2024.

31 Nvidia, 2024, Large Language Models Explained, https://www.nvidia.com/en-us/glossary/large-language-models/#:~:text=Large%20language%20models%20(LLMs)%20are,content%20using%20very%20large%20datasets.

32 American Library Association, 2018, “Media Literacy,” www.ala.org/aasl, retrieved June 19, 2024.

33 American Institutes for Research, 2023, “Essential Components of MTSS,” https://mtss4success.org/essential-components#:~:text=A%20multi%2Dtiered%20system%20of,from%20a%20strengths%2Dbased%20perspective.

34 Urban Dictionary, 2024, Urban Dictionary: Negging.

35 Hobbs, R., Chapman, D., Doerr-Stevens, C., et al., April 9, 2022, "Media Education in English Language Arts," National Council of Teachers of English, https://ncte.org/statement/media_education.

36 Center on Positive Behavioral Interventions & Supports, 2023, "What Is PBIS?" www.pbis.org., www.pbis.org/pbis/what-is-pbis.

37 White, S., Scott, A., Koshy, S., January 18, 2024, "Responsible AI & Tech Justice: A Guide for K-12 Education," Kapor Foundation, https://kaporfoundation.org/wp-content/uploads/2024/01/Responsible-AI-Guide-Kapor-Foundation.pdf, used with permission as provided through CC BY-ND 4.0, Attribution-NoDerivatives 4.0 International, Creative Commons License, http://creativecommons.org/licenses/by-nd/4.0/, retrieved August 20, 2024.

38 Enriching Students, 2021, "RTI vs. MTSS," Interval Technology Partners, LLC, https://www.enrichingstudents.com/rti-vs-mtss/.

39 Qi, J., Yan, Y. & Yin, H., April 19, 2023, "Screen Time Among School-Aged Children of Aged 6–14: A Systematic Review," *Global Health Research and Policy*, 8, 12. https://doi.org/10.1186/s41256-023-00297-z.

40 Center for Teaching Innovation, 2024, "Cornell University Centre for Teaching Excellence," www.cte.cornell.edu, retrieved May 2024.

41 Punie, Y., Redecker, C., editor(s), 2017, "European Framework for the Digital Competence of Educators: DigCompEdu," EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 2024.

42 Schuetz, R., December 1, 2014, "Self-Directed vs. Self-Determined Learning; What's the Difference?" www.rtschuetz.net/2014/12/self-directed-vs-self-determined.html, retrieved May 2024.

43 Brookfield, S. D., 1994. "Self-Directed Learning," in YMCA George Williams College ICE301 Lifelong learning, Unit 1 Approaching lifelong learning. London: YMCA George Williams College. Available in the informal education archives. https://infed.org/mobi/self-directed-learning/, retrieved, May 28, 2024.

44 Punie, Y., Redecker, C., editor(s), 2017, "European Framework for the Digital Competence of Educators: DigCompEdu," EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 27, 2024.

45 Patchin, J., & Hinduja, S., 2018, "Sextortion Among Adolescents: Results from a National Survey of U.S. Youth," *Sexual Abuse: A Journal of Research and Treatment*, 32. https://doi.org/10.1177/1079063218800469, retrieved June 7, 2024.

46 Cheng, L., & Varshney, K., March 14, 2024, "Socially Responsible AI Algorithms: Issues, Purposes, and Challenges," https://ar5iv.labs.arxiv.org/html/2101.02032.

47 NIST, January 21, 2020, "Trustworthy AI: A Q&A with NIST's Chuck Romine," www.nist.gov/blogs/taking-measure/trustworthy-ai-qa-nists-chuck-romine.

48 Punie, Y., & Redecker, C., editor(s), 2017, "European Framework for the Digital Competence of Educators: DigCompEdu," EUR 28775 EN, JRC Science for Policy Report, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-73718-3 (print), 978-92-79-73494-6 (pdf), doi:10.2760/178382 (print), 10.2760/159770 (online), JRC107466, retrieved May 27, 2024.

49 VOLUNTEER | English meaning – Cambridge Dictionary.

Taylor & Francis
Taylor & Francis Group
http://taylorandfrancis.com

Index

Note: **Bold** page numbers refer to tables and *italic* page numbers refer to figures.

ableism 440
academic pressure **327**
acceptable behavior 90–92, 130–133
Acceptable Use Policy (AUP) 440
accessibility 440
access to reliable news **327**
acute trauma 37
adaptive learning 81, 440
adaptive lessons 441
Adolescent Brain Cognitive Development^{SM} Study 38
adult sexual misconduct (ASM) 233, 269
advocate 35, 45, 50, 295, 300, 312, 441
AI *see* artificial intelligence (AI)
AIED *see* Artificial Intelligence in Education (AIED)
algorithm 80, 299, 441
algorithm bias 441
algorithmic discrimination 441
algorithmic literacy 441
American Academy of Child and Adolescent Psychiatry 194
amoral 23
Angelini, G. 267
ANNs *see* Artificial Neural Networks (ANNs)
anti-bullying 35
Anti-Bullying Laws, Policies, and Regulations 42
The Antisocial Network: Memes to Mayhem 267, 269
AP Computer Science A 395
Apple screen time app **196**
App Review
  cyber safety through 398
  of mobile device 399
    Android Phone 402–404
    Apple iPhone 400–402
apps
  considered dangerous for seventh- and eighth-grade students 399
  downloading without permission 195
  identifying risky apps on child's device 398–404
  monitoring software 379–381
  questionable 378–379
  risky 376–378
  for seventh- and eighth-grade students 398–399
  websites 375–376
Ardern, J. 315
artificial intelligence (AI) 17, 54–55, 128–129
  activity: AI ethics role-play 75
  applications 83
  avoiding bias in 74
  bill of rights 396

artificial intelligence (AI) (*cont.*)
  challenges and considerations for educators 59–60
  in classroom
    enhancing learning experiences 58–59
    preparing students for future 58–59
  classroom discussion and exercise 73–74
  concepts and capstone project 85–86
  in daily life 74
  in education
    and pedagogy 84–85
    toolkit for racial equity 393
  ethical framework 394
  ethical use of 72–74
  framework 392
    and guidance educators 393–397
    and libraries benefit users 392–393
  functional overview *66*
  fundamentals 63–64
  and future of teaching and learning 394
  guidance for schools toolkit 393
  hallucinations 70
  literacy for educators 80–83, **82**
    one-year education plan of study 83–86
  literacy framework 395
    ask, adapt, author, analyze 396
  in modern education 88
  power of AI in fake news 217
  privacy and data protection 74
  responsible AI and tech justice 60–61
  risks 69
  role in everyday life 58
  socioeconomic benefits 72, *73*
  teaching AI systems 64
  tools 354–357
    and basic programming 84
  training 65
    step-by-step approach 66–68, *67*
  transparency and understanding AI decisions 74
  unethical uses of 70–72, *72*
  usage in education 60, *60*
  using AI *vs.* abusing AI 86, **87**
Artificial Intelligence in Education (AIED) 85, 86, 441
Artificial Intelligence (AI) literacy 441–442
Artificial Neural Networks (ANNs) 64
ASM *see* adult sexual misconduct (ASM)
AUP *see* Acceptable Use Policy (AUP)
Aura app **196**
authentic learning experiences 442
autism 261, 442
avatar 265
avatar safety, gaming and 263, 274–275

badges
  digital badge, conceptual designs 389–391
  ideas 388–389
  websites 386–387
Bark app **196**
behavior 442
  acceptable 90–92, 130–133
  anti-bullying 35
  cyber-safe, leadership and fostering 20–22
  online cyber-secure 22
"Be Internet Awesome" website **325**
belittlement 442
"Ben Doe ben.doe@sony.com" 424
Berkley, M. 262
biblical stewardship **294**
biodiversity 442
bioregion 297, 442
blended learning 442
body image and self-esteem **327**
BrainPOP Jr. Internet Safety Video 353
Breachsense 410, *410*
bullying 35–38; *see also specific types*
  anti-bullying 35
  cyberbullying *see* cyberbullying
  disability 39, 101–102, **107**, 139–141
  emotional 39, 103–104, **107**, 142–145
  hate generated 36, *37*
  personal 40, 105–109, **107**, 146–148
  physical 40, **107**, 110–111, 149–152
  racial 40, **107**, 112–116, 153–156
  religious 40, **107**, 117–121, 157–160
  school 41
  social 40–41, **107**, 122–123, 162–163
  verbal 41, 43, **107**, 124–127, 164–166

carbon dioxide 302
carbon emissions 302
Carson, R. 296
Center for Creative Leadership (CCL) 6
  DAC model for leadership 6
Center for Parent and Teen Communication 53

Centers for Disease Control and Prevention (CDC) 261, 454
  National Vital Statistics System 270
  suicide rates 270
certificates
  ideas 388–389
  websites 387–388
character development in individuals 3–5
character education 1
  civic and global responsibility 2
  class student credo creation 4–5
  community involvement 3
  components of 2–3
  connecting to broader community 5
  core values 4
  definition 2–3
  ethical decision-making 2
  importance of 1–2
  media and internet influence 4
  ongoing conversations and support 5
  positive behavior reinforcement 2
  recognizing and celebrating character 5
  reflecting on personal growth 5
  relating values to everyday life 4
  resilience and perseverance 2
  role modeling 3
  role-playing activities 4
  social and emotional learning 2
  values and virtues 2
"Children and Parents: Media Use and Attitudes" report (2023) 190
Children's Online Privacy Protection Act (COPPA) 268
child sexual exploitation and abuse 443
Choi, M. 307, *307*, 309–312
chronic trauma 37
CISA *see* Cybersecurity and Infrastructure Security Agency (CISA)
citizenship, digital *see* digital citizenship
classroom discussion 233
clickbait **218**, 443
Coffey, A. 7, 8
cognitive development 443
cohesiveness 443
collaborative problem-solving 318
Common Components in State Anti-Bullying Laws 42
Common Sense Media's Census program 324
common sense media website **325**
communication
  digital literacy and 310, 311
  skills 11
community involvement, character education 3
community stewardship **294**
complex PTSD (CPTSD) 37
computer type 443
The Com 235
conformity 443
confronting tech power 397
Conradt, M. 425
conservation stewardship 294
conspiracy theory 444
continous professional education (CPD) 443
control of institutions 444
conversations and support 32
COPPA *see* Children's Online Privacy Protection Act (COPPA)
corporate social responsibility (CSR) stewardship **294**
counterfactual 49, 444
CPD *see* continous professional education (CPD)
Crabtree, M. 77
Crawford, M. 37
critical resistance (CR), digital citizenship as 308
critical thinking 88, 221, 444
  and active participation 311
  building digital literacy and 56–57
  digital literacy and 59
  encourage 79–80
  and problem-solving 33
CSR stewardship *see* corporate social responsibility (CSR) stewardship
cultural stewardship **294**
cyber attacker's approach 406–407
cyberattacks against consumers 406
  cyber attacker's approach 406–407, 412–414
  data breach databases and notification services 410–412, *410–412*
  digital footprints
    data breaches 410
    deleting unwanted data *409*, 409–410
    Google yourself 408
    wayback machine (Internet archive) 408

cyberattacks against consumers (*cont.*)
  phishing and social engineering attacks 412–413
  psychology behind phishing emails 414–415
  safe social media practices 408
  self protection 407–408
  spoofing *vs.* phishing 415–416
    dealing with online strangers 416
    email domain check 418–423, *419–423*
    email verification services 424–425
    using OSINT techniques 416
    validate social media profile 416–417
    verifying works at company 418
cyber-aware 178
Cyber Awareness & Safety Education (CASE) 358
cyberbullying 39, 97–100, **107**, 137–138, **327**, 444
  avoiding 28–29
  awareness and prevention 184
  and digital etiquette **298**
  risks *39*
cyber footprint, monitoring 211
cyber grooming 233, 265, 429
cyber risks 35, 178, 407
cyber-safe 208–210
  behavior, leadership and fostering 20–22
  culture 21
  online experience 195–196
  skill 178
cyber safety 19–20, 27, 243–250, 325–326
  good character for 5, **6**
  long-term 62
  maintaining a proactive position on 34
  and online world 428–429
    proactive support 429
    reactive/supportive responses 431
    warning signs and assessment 430–431
  reinforces ethics 27–28
  skills for 33–34
  through App Review 398
  trust enhances 27
cyber-secure behavior, online 22
cybersecurity
  awareness 234
    recommendations 235–236
  global information resources **236**
  literacy 33
Cybersecurity and Infrastructure Security Agency (CISA) 208
Cyber Smart 179
cyberspace 26, 299, 300, 324, 444
cyberstalking 444
cyber stewardship 299–303, 325–326
  fostering online responsibility 314–315
  practical application for classroom 300–303
cyber threats, mitigating hacking and 326

DAC model *see* Direction, Alignment, and Commitment (DAC) model
Daniels fund ethics 51, *52*
data breaches
  databases and notification services 410–412, *410–412*
  reduces impact of 199–200
data-driven decision-making 17
data literacy 445
data point 65, 445
data privacy **298**
  and security 19
data science *64*
data security and privacy 19
deaf-blindness 447
decision-making
  data-driven 17
  ethical judgment and 33
  healthy 53
  judgment and 46–47
deepfakes 71, 217, **218**, 219–238, 445
  mitigate the risks of 220
  usage 219, **219**
deep learning (DL) 63, 65, 445
Defining and Measuring Youth Digital Citizenship (Jones and Mitchell) 306
deforestation 323, 445
demonstrate leadership qualities 318
demonstrate leadership skills, in online communities 316
Department of Homeland Security (DHS), US 208
  Digital Safety Series 264
developmental delay 447
digital age
  environmental stewardship in 328
  leadership in 34

digital badge, conceptual designs 389–391
digital behavior, comprehensive framework for 310–311
digital citizen 249, 250, 305, 307, 310, 315, 318, **389**, **391**, 445
digital citizenship 240–242, 305–306, 445
  Choi's four categories of 307, *307*
  as critical resistance 308
  development of responsible digital habits 311
  educate **309**
  education in classroom 312–313
  empowering students through 309–312
  empowering students to use voices for good 312
  ethical and safe use of technology 311
  as ethics 307
  fostering online responsibility 314–315
  frameworks for 307
  implications for education and educator 308–309
  as Media and Information Literacy (MIL) 308
  as participating/engagement (P/E) 308
  promoting critical thinking and active participation 311
  protect **309**
  relevant to 21st-century students 312
  respect **309**
  Ribble's and Choi's frameworks 309–312
  Ribble's nine elements of 309, **309**
digital civics 445
digital collaboration tools 317
digital competence 446
digital competitiveness 446
digital content 211, 215, 221, 234, 310, 311, 319, 446
digital creativity 446
digital decay 211, **212**, 446
digital dependency, society 315
digital etiquette, cyberbullying and **298**
digital footprints 210–211, **212**, **298**
  data breaches 410
  deleting unwanted data *409*, 409–410
  Google yourself 408
  wayback machine (Internet archive) 408
digital hygiene practices 33
digital intelligence (DQ) 446
digital leaders, traits of effective 315–316
digital learning *see* online learning
digital literacy 233–234, 303–305, 328, 446
  and adaptability 18
  advocating for 299
  and communication 310, 311
  and critical thinking 56–57, 59
  empowering middle school students through 305
  leadership 19
  maintaining 19
  and online safety 327
  skills 88
digital natives 446
digital rights, privacy and 318
digital safety 264, 311
digital social networking (DSN) 192
  risks of 228–233
digital stewardship 336–337, 342–343, 446
digital use divide 447
Direction, Alignment, and Commitment (DAC) model 6, *7*
disability 447
  bullying 39, 101–102, **107**, 139–141
  children with 261, 447
  multiple 454
discrimination, algorithmic 441
disordered eating habits 430
dissing 447
diversity and inclusion **328**
DKIM 421, *422*, *423*
DMARC 421, *422*, 423
dogpiling 447
doxing/doxxing 264, 447
Doyle, N. 40
DQ *see* digital intelligence (DQ)

Earth Day *322*, 322–324
EDI *see* Equality, Diversity, and Inclusion (EDI)
education and awareness 326
educator 5, 8–10, 13, 20, 25, 28, 30, 33, 57–59, 62, 448
  AI framework and guidance 393–397
  AI literacy for 80–83, **82**
  digital citizenship implications for education and 308–309
  takeaways from scenario activity 208
EEPDI *see* Environmental Education Professional Development Institute (EEPDI)

e-learning *see* online learning
elementary school 448
email verification services 424–425
embracing technology 19–20
emerging technologies 237–238
emissions, carbon 302
emotional bullying 39, 103–104, **107**, 142–145
emotional disturbance 448
emotional regulation 448
empathy 32, 34, 102, 103, 139, 146
  and emotional intelligence 12
encryption 448
energetic play 448
environmental awareness **328**
Environmental Education Professional Development Institute (EEPDI) 296
environmental stewardship **294**, 340–341, 346–347
  in digital age 328
  pioneers of 295–297
environmental sustainability *322*
Epic! website **325**
Equality, Diversity, and Inclusion (EDI) 29
equity 449
  and access 59
  racial
    AI in education toolkit for 393
    through tech policy 396
ESET parental control app **196**
ethical decision-making, character education 2
ethical judgment and decision-making 33
ethical leadership 29
  classroom discussion on 30–31
  Lo Iacono's eight traits of 29, *30*
Ethical Leadership: A Cornerstone of Success in Business and Effective Managerial Training (Lo Iacono) 29
ethical standards 25–26
ethical stewardship **294**
ethical use of technology 227
ethics 448
  and artificial intelligence 168–173
  in context of cyber safety 27
  core principles of 23, *26*
    ethical standards 25–26
    judgement 24
    morals 23–24
    norms 24–25
    values 23
  digital citizenship as 307
  in digitally connected world 34
  and leadership 28, 93–96, 134–136
    mutualistic relationship 28–29
    respecting privacy 28
    sharing accurate information 29
European Union (EU) 16
executive function 268, 449
EXIF (Exchangeable Image File Format) metadata 190

fair use 319
fake news 449
  creators 449
  disinformation types 217, **218**
  on Instagram *215*, 243
  and media 213
  and misinformation 217
  power of AI in 217
  purveyors 449
  in social media 216
Family Planning NSW 261
FamiSafe app **197**
Federal Bureau of Investigation (FBI) 263, 266, 272
Films and Publications Amendment Act, 2009 (South Africa) 231
Films, Videos, and Publications Classification Act 1993 (New Zealand) 230
financial stewardship **294**
flaming 40, 449
food insecurity awareness **328**
footprint
  cyber, monitoring 211
  digital 210–211, **298**
fraping 449

gamers 265, **377–379**, 449
gaming 449
  and avatar safety 263, 274–275
  and online safety 282–283
GAO *see* Government Accountability Office (GAO)
gaslighting 38, 449

genAI *see* generative artificial intelligence (genAI)
gender identity 450
Generation (Gen) Alpha 35, 295–297, 450
  adaptability and resilience 50
  attention span 50
  diverse 49
  environmentally conscious 50
  make decisions 49–54
  tech-savviness 49
generation beta/gen beta 450
generative artificial intelligence (genAI) *55*, 55–56, 76, 450
  literacy 76–77, *78*, 449–450
    educational process 79–80
  models 69
  role in education 56–57
  tools 57, **57**, 354–357
Gen Z 49
  social media users 187–188
GeoImgr app **190**
Georgia Public Broadcasting (GPB) 353–354
GeoSetter app **190**
German Criminal Code 230
Gmail 418, *419*, 420, *420*, *423*
good character
  courage **6**
  for cyber safety 5, **6**
  defining 2
  integrity **6**
  leadership and 22–23
  respect **6**
  responsibility **6**
good judgment 48–49
good leader, attributes of 7–8
Google Family Link tool 196
Government Accountability Office (GAO) 36, *36*, 41, 269
grade 7, lesson plans 90–129, 240–248, 274–281
  acceptable behavior 90–92
  artificial intelligence 128–129
  cyberbullying 97–100
  cyber safety 243–248
  digital citizenship 240–242
  disability bullying 101–102
  emotional bullying 103–104
  environmental stewardship 340–341
  ethics & leadership 93–96
  gaming and avatar safety 274–275
  personal bullying 105–109, **107**
  physical bullying 110–111
  racial bullying 112–116
  religious bullying 117–121
  social bullying 122–123
  stewardship 334–339
  tricky person 276–281
  verbal bullying 124–127
grade 8, lesson plans 130–173, 249–254, 282–290
  acceptable behavior 130–133
  cyberbullying 137–138
  cyber safety 251–254
  digital citizenship 249–250
  disability bullying 139–141
  emotional bullying 142–145
  environmental stewardship 346–347
  ethics and artificial intelligence 168–173
  ethics & leadership 134–136
  gaming and online safety 282–286
  personal bullying 146–148
  physical bullying 149–152
  racial bullying 153–156
  religious bullying 157–160
  social bullying 162–163
  stewardship 334–335, 342–345
  tricky person 287–290
  verbal bullying 164–166
graph-based algorithms 216
greenhouse effect 302
grooming (cyber grooming) 233, 265, 429, 450
  sexual 443
group projects and discussions 31

hacking 40, 326–327, 450
harassment 36, 41, 42, **187**, 231, 306, 450
hate generated bullying 36, *37*
HaveIBeenPwned 410–412, *411*
Haynes-Tross, E. 9, 12
health impairments 456
healthy decision-making 53
healthy social media
  vs. unhealthy social media 186
  vs. unhealthy social networking **187**
hearing impairment 102, 450
Hero1985 413

Herold, B. 213
High-Level Machine Intelligence (HLMI) 75–76, *76*, 451
homeschool students 451
Honey Badger *see* Generation (Gen) Alpha
human–computer interaction 61, 451
Hunter.io 424
hyperpartisan websites 451

IDEA *see* Individuals with Disabilities Education Act (IDEA)
identity politics 451
identity theft 27, 179, 180, 192, 200, 415, 451
immoral 23
impersonation 99, 452
Incogni 410
individualized learning 452
Individuals with Disabilities Education Act (IDEA) 452
information disorder 451
information literacy 213, 451
  reaching and teaching students about 222
information steward 452
Information Technology Act, 2000 (India) 230
intellectual disability 261, 452
intellectual property 318–319
interactive lessons 328, 452
Internet Matters 260
Internet safety 241, 306, 314, 326, 350, 357, 359, 362, 452
intimidation 152, 452

Jones, A. 267
Jones, L. M. 306
judgement 24
  and decision-making 46–47
  good 48–49
JustDeleteMe website *409*, 409–410

Kapor Foundation 61
Kaspersky safe kids app **197**
K—12 education 60, 393–397
  advanced placement CS principles 395
  computer science
    content standards 394
    teacher standards 394
Kik app 188
  risks associated with **189**
Kik Messenger (Kik) 399
Killing Pig Plate 204

large language models (LLMs) 453
Laursen, B. 47
Lavery, S. 7, 8
law, sexting and 229–231
LCSW 35, 37
leaders
  effective 9
  role modeling 21
leadership 10
  in action 11
  capabilities, technology enhancements 17
  CCL's DAC model for 6, *7*
  collaborative efforts and teamwork 21
  communication and education 20
  crisis management and incident response 20
  data privacy and security 19
  definition 6–7
  development 7
  in digital age 19–20, 34
  digital literacy 19
    and adaptability 18
  empathy and emotional intelligence 12
  ethical standards and integrity 20
  and fostering cyber-safe behavior 20–22
  goal-setting workshop 12
  and good character 22–23
  human connection
    fostering 18
    maintaining 18
  importance of collaboration in 317
  opportunity tasks for middle school students 12, **12–13**
  personal leadership qualities 10–11
  qualities, demonstrate 318
  reflecting on leadership experiences 11
  responsibility and accountability 20
  role modeling 21
  with seventh- and eighth-grade students 8–10
  strategic thinking and risk management 20
  teaching 19–20
  technology and 17–20
  transformational 9
leadership attitude
  effect on development of 15–16

  global social context and development of 15–16
leadership roles
  engaging middle school students in 13–14
  guiding class discussion 13
  learning in multiage classrooms 13
  participation in team sports/activities 14
  pursuing personal projects 14
  serving the community 13–14
leadership skills
  communication skills 11
  development 11
  in online communities 316
  teaching 9–11
learning
  individualized 452
  project-based 458
  self-determined 460
  self-directed 460
  self-regulated 460–461
lesson plans
  grade 7 90–129, 240–248, 274–281
  grade 8 130–173, 282–290
Lewis, J. 324
literacy
  algorithmic 441
  data 445
  digital *see* digital literacy
LLMs *see* large language models (LLMs)
Lo Iacono, V. 29

machine learning (ML) 64, 65, 453
malinformation **218**, 453
Malware 201, 209, 232, 235, **298**, 453
  and viruses **298**
mandatory reporters 268–269
masquerading *see* impersonation
McCarthy, J. 54
mean girl behavior 38, 453
Media and Information Literacy (MIL), digital citizenship as 308
media, fake news and 213–244
media literacy 221, 233, 234, 310, 453
  Choi's emphasis on 311
  reaching and teaching students about 222
  skills 220, 311
  social 191
  teach online and social 429
mental health
  awareness **328**
  teen well-being and 269–272
mentor 54, 296, 297, 453
metabolic equivalent of task (MET) 453
Microsoft family safety app **197**
middle school 20, 453
middle school students
  leadership opportunity tasks 12, **12–13**
  leadership roles 13–14
  teaching ethical leadership to 30
  through digital literacy 305
MIL *see* Media and Information Literacy (MIL)
Minecraft education edition website **325**
Minsky, M. 55
misleading information 213, 454
Mitchell, K.J. 306
ML *see* machine learning (ML)
Mobicip app **197**
mobile device, App Review of 399
  Android Phone 402–404
  Apple iPhone 400–402
morals 23–24
multiple disabilities 454
multi-tiered system of supports (MTSS) 454
mutualistic relationship between ethics, trust, and cyber safety 27–28

National Alliance on Mental Illness (NAMI) 354
National Association for Media Literacy Education (NAMLE) 221
National Center for Missing & Exploited Children (NCMEC) 266, *267*
National Council of Teachers of English 306
National Institutes of Health (NIH) 38
National Science and Teaching Association's Environmental Education Professional Development Institute (EEPDI) 296
National Science Teaching Association (NSTA) 296
National Vital Statistics System, CDC 270
Natural Language Processing (NLP) 63
NCDIT *see* North Carolina Department of Information Technology (NCDIT)

NCEI *see* nonconsensual explicit imagery (NCEI)
NCMEC *see* National Center for Missing & Exploited Children (NCMEC)
negging 454
networking practices, social media and 184–185
neural networks 64, 65, 217, 356, 445, 454
neuroscience 454
Neuroscience News 48, 49
Newport Academy 38
news literacy 454
Next Generation Science Standards (NGSS) 296
NGSS *see* Next Generation Science Standards (NGSS)
Nilsen, S. 428, 432
Nintendo Switch 408
NLP *see* Natural Language Processing (NLP)
nonconsensual explicit imagery (NCEI) 454
nonconsensual pornography 229, 454
non-screen-based sedentary time 455
norms 24–25, 148, 455
North Carolina Department of Information Technology (NCDIT) 183
Norton family app **197**
NSTA *see* National Science Teaching Association (NSTA)

OECD *see* Organisation for Economic Co-operation and Development (OECD)
OmeTV 399
online behavior, setting rules for 325
online communities, demonstrate leadership skills in 316
online cyber-secure behavior 22
online enticement 233
online environment safe 325, **325**
online learning 303–305, *304*, 455
online privacy
  and personal data protection 179
    beware of public wi-fi 182–183
    HTTPS security 181
    maintenance 183–184
    oversharing 179–180
    privacy settings check 181
    recommendations 180–183
    use secure apps and websites 181
  and safety **328**
online recruiter 263, 455
online respect and perspective-taking 313–314
online safety
  digital literacy and 327
  gaming and 282–286
openly licensed educational resources 455
open-source intelligence (OSINT) 406, 416, 455
Oregon Department of Education 303, 305
Organisation for Economic Co-operation and Development (OECD) 15, 455
orthopedic impairment 455
OSINT *see* open-source intelligence (OSINT)
outcomes 456
outing *see* trickery
oversharing on social media **298**

parental controls and open dialogue 193–194
  conversation 194–195
  cyber-safe online experience 195–197
  downloading apps without permission 195
participating/engagement (P/E), digital citizenship as 308
Paska, L. 213
passphrase 19, 22, 198, 456
password 456
password hygiene 456
password-related attacks, risk of 199
password security **298**
password security and account protection 197–198
  enable two-factor authentication 198–199
  strong passwords 198
PBIS *see* positive behavioral interventions and supports (PBIS)
peer influence 47, 194, 456
peer pressure 88, 96, 192, 456
  influence 47
  susceptibility 47
  on trip 136
peer susceptibility 47, 456
permissive reporter 269
personal bullying 40, 105–109, **107**, 146–148
personal data protection, online privacy and 179
  beware of public wi-fi 182–183
  HTTPS security 181

  maintenance 183–184
  oversharing 179–180
  privacy settings check 181
  recommendations 180–183
  use secure apps and websites 181
personalized learning 56, 58, 72, 81, **87**, 327, 457
personal leadership qualities 10–11
personally identifiable information (PII) 268
personal private information (PPI) 198
pervasive computing 457
pervasive education 457
pervasive technology 457
Pew Research Center 210–211
phishing 457
  protection against, 2FA 200
  and social engineering attacks 412–413
phishing emails
  authority 414
  curiosity 415
  familiarity and trust 414
  greed and excitement 414
  psychology behind 414–415
  urgency and fear 414
phishing scams **298**
  darker side of 203, *203*
  recognizing and avoiding 200
  10 "red flags" 201–202, *202*
phishing *vs.* spoofing 415–416
  dealing with online strangers 416
  email domain check 418–423, *419–423*
  email verification services 424–425
  using OSINT techniques 416
  validate social media profile 416–417
  verifying works at company 418
Photo investigator app **190**
physical bullying 40, **107**, 110–111, 149–152
Picarta.ai app **190**
Pic2Map app **190**
pig butchering scam 204–205, *206*, 457
PII *see* personally identifiable information (PII)
piracy and illegal downloads **298**
plagiarism 319
PlayStation Network (PSN) 408
Policies and Regulations 42
pop-up blockers 267
pornography, nonconsensual 229, 454
positive behavioral interventions and supports (PBIS) 457
positive behavior reinforcement, character education 2
post-traumatic stress disorder (PTSD) 37
PPI *see* personal private information (PPI)
Pratt, J. 306
predator 266, 458
  sexual 266, 461
prekindergarten 458
preschool 432, 458
Preventing and Promoting Relationships & Eliminating Violence Network (PREVNet) 38
privacy and data, protection 326
problem-solving
  critical thinking and 33
  technology for collaborative 318
project-based learning 458
Protection from Harassment Act (2014) 231
ProtonMail 418, *419–422*, 420
psycho-education 429, 458
PTSD *see* post-traumatic stress disorder (PTSD)
public charter school 458
public Wi-Fi safely use **298**
puzzle, stewardship word find *331*, *332*

questionable apps 378–379
quishing 458
Qustodio app **197**

racial bullying 40, **107**, 112–116, 153–156
racial equity
  AI in education toolkit for 393
  through tech policy 396
RAI *see* responsible AI (RAI)
Readiness and Emergency Management for Schools (REMS) 268
recommended readings 366–372
reflective journaling 31
reinforces ethics, cyber safety 27–28
religious bullying 40, **107**, 117–121, 157–161
REMS *see* Readiness and Emergency Management for Schools (REMS)
repurpose 458

resilience and perseverance, character education 2
response to intervention (RTI) 459
responsible AI (RAI) 60
  and tech justice 60–61, 458
Responsible AI and Tech Justice Guide for K—12 Education 61
The Responsible AI and Tech Justice Guide for K—12 Education 61
Responsible Artificial Intelligence (RAI) Toolkit 397
revenge porn 229, 454, 459
Ribble, M. 307, 309–312
Rich, E. 54
Rikki Turner, Ed.D. 435–436, *436*, 438
risk 459
  apps 376–378
  artificial intelligence 69
  assessment 459
  associated with Kik app **189**
  cyberbullying *39*
  of digital social networking 228–233
  management 20, 34, 459
  mitigate the risks of deepfakes 220
  of password-related attacks 199
  potential risks of social media 187
role 459
  artificial intelligence role in everyday life 58
  in education 56–57
  Generative AI (GEN-AI) role in education 56–57
  leadership 13–14
role modeling
  character education 3
  leaders 21
  leadership 21
role models, guest speakers and 31–32
role-playing activities, character education 4
role-playing exercises 31
RTI *see* response to intervention (RTI)
rumors in social media 216

safe adult 262
SAFE benchmarks framework 395
safe *vs.* unsafe people 287
safe-word 271–272
San Bernardino Sun (CA) reports 44
satire **218**, **219**, 459
ScatteredSecrets 411, *411*, 412, *412*
Scattered Spider 234
school bullying 41
Schumacher, M. 428, 432
Science, Technology, Engineering, and Mathematics (STEM) 459
Scratch website **325**
screen time 460
  defining *223*, 223–225, *224*
  impact of 222–245
  recommendations for monitoring and managing 226–227
Screen time app **197**
search engine optimization (SEO) 354
  tools 212
secondary/high school 460
secondary trauma 37
security, data privacy and 19
sedentary screen time 460
self-assessment 460
self-assessment tool 460
self-determined learning 460
self-directed learning 460
self-harm behaviors 430
self-harm warning signs 431
self-regulated learning 460–461
SEO *see* search engine optimization (SEO)
seventh- and eighth-grade students
  apps considered dangerous for 399
  apps for 398–399
  ethical principles for 32–33
  leadership with 8–10
  suicide—well-being and mental health 435–436, **437–438**
  value and importance of responsible AI 62–63
sexting 228–229, 461
  and law 229–231
  students at risk 232
sextortion 203, 228, 229, 232, 233, 266–270, 428, 434, 461
sexts 461
sexual predator 266, 461
shallowfakes 461
Sha Zhu Pan 204
SIFT framework *214*, 213–216
simulated neural networks 64
skills for cyber safety 33–34

SMDS *see* Social Media Disorder Scale (SMDS)
SMiShing 461
Snapchat 398
social and emotional learning 2, 461
  character education 2
social bullying 40–41, **107**, 122–123, 162–163
social context, influence on 16
social engineering **298**
  tactics 33
social issues through technology 327, **327–328**
social media 184, 373, 461–462
  cyber-safe practices 189
  healthy *vs.* unhealthy 186
  identifying hoaxes, fake news, and rumors in 216
  impact 186–188
  and networking practices 184–185
  oversharing on **298**
  potential risks of 187
  research sources 381–384
  safer for students 188–192, **190**
  safe social media practices 185–186
  vs. social networking 184, **185**
Social Media Disorder Scale (SMDS) 430
social media practices, safe 408
social media use 186, 187, 191, 430
social networking 184, 192–193, 373, 462
  digital, risks of 228–233
  research sources 381–384
  risks 192, **193**
  vs. social media 184, **185**
social responsibility of AI 462
society's digital dependency 315
software updates and patches **298**
spear phishing 462
specific learning disability 462
speech/language impairment 462
SPF 421, *422*
Spokeo Social Search 416
spoofing *vs.* phishing 415–416
  dealing with online strangers 416
  email domain check 418–423, *419–423*
  email verification services 424–425
  using OSINT techniques 416
  validate social media profile 416–417
  verifying works at company 418
"Start Talking: A Guide to Keeping Children Safe Online" 211
STEM *see* Science, Technology, Engineering, and Mathematics (STEM)
"steward of cyberspace" 299
steward of relationships 320–321
stewardship 293–294, 334–339, 342–345
  cyber 299–303
  environmental, pioneers of 295–297
  of influence 319–320
  of students 319
  teacher's role 319
  technological and data 297, **298**
  teens' daily routines 295–297
  types **294**, *294*
  word find puzzle *331*, *332*
"Stewardship, Security, and Cyberspace" (Lewis) 324
StopBullying.gov. 42
stop cyberbullying 326
students
  digital citizens, empowering 179
  discussion and engagement, scenario design 207–208
  leadership opportunities, creation 12, **12–13**
  stewardship of 319
suicidal ideation 430
suicide rates, CDC 270
suicide, well-being and mental health for Grades 7 & 8 435–436, *436*, **437–438**
Sundar Pichai 316
Sweeney, B. 266

teacher's resource list
  blogs 351
  CBS news video resources — online scams 351–352
  children's illustrated books 352
  crisis and intervention 352
  cyber safety research 352–353
  digital resources 353–357
  instructional resources 357–358
  interactive assessment exercises 358
  interactive games and classroom exercises 358–359

teacher's resource list (*cont.*)
  NPR video resources 359
  podcasts 359–360
  publications 360
  TED-Ed video resources 361
  web sites 362–364
  YouTube/Netflix video resources 361–362
teaching
  ethical leadership to middle school students 30
  leadership 19–20
  leadership skills 9
    to students in seventh and eighth grade 10–11
  transitioning from monitoring to 178
technology and leadership 17–20
"threat actor" 180
TikTok 399
time management **328**
TinEye app **190**
transformational leadership 9
trauma 37
  acute 37
  chronic 37
  secondary 37
traumatic brain injury 463
tribal colleges and universities 463
trickery 463
tricky person 260–261, 287–290
trolling 463
trust, enhances cyber safety 27
trustworthy artificial intelligence 463
two-factor authentication (2FA) 197–199
  enhanced security 199
  protection against phishing 200
  recommendations for implementing 199–200

ubiquitous computing 457
UNESCO *see* United Nations Educational, Scientific and Cultural Organization (UNESCO)
unhealthy social media *vs.* healthy social media 186
unhealthy social networking *vs.* healthy social media **187**
United Kingdom's Office of Communications (Ofcom) reporting (2023) 225
United Nations Educational, Scientific and Cultural Organization (UNESCO) 15–16, 41
US Department of Homeland Security 208
US Federal Law Section 2251 of Title 18 229
US Government Accountability Office (GAO) 36, *36*, 269
US territories 42

values 23
verbal bullying 41, 43, **107**, 124–127, 164–167
Verify Email Address 424
virtual learning environment (VLE) 463
virtue 2, 5, 51, 78, 463
vishing 464
visual impairment 141, 463
VLE *see* virtual learning environment (VLE)
Voila Norbert 424
volunteer 321, 463
vulnerabilities 34, 192, 211, 406, 464

warning signs and assessment, cyber safety 430–431
The Wayback Machine 264
Weber, M. 2
websites 374–375
  app 375–376
  badges 386–387
  certificates 387–388
  harmful **325**
  hyperpartisan 451
WebWatcher app **197**
whaling 464
Whitson, L. 44
WHOIS 181